# Graduate Texts in Mathematics

Benson Farb
R. Keith Dennis

# Noncommutative Algebra

Springer-Verlag

Graduate Texts in Mathematics 144

# Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFFER. Topological Vector Spaces.
4 HILTON/STAMMBACH. A Course in Homological Algebra.
5 MAC LANE. Categories for the Working Mathematician.
6 HUGHES/PIPER. Projective Planes.
7 SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiometic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
14 GOLUBITSKY/GUILEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
20 HUSEMOLLER. Fibre Bundles. 2nd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra. Vol. I.
29 ZARISKI/SAMUEL. Commutative Algebra. Vol. II.
30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 WERMER. Banach Algebras and Several Complex Variables. 2nd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to $C^*$-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.

*continued after index*

Benson Farb
R. Keith Dennis

# Noncommutative Algebra

With 13 Illustrations

Springer Science+Business Media, LLC

Benson Farb
Department of Mathematics
Princeton University
Fine Hall, Washington Road
Princeton, NJ 08544
USA

R. Keith Dennis
Department of Mathematics
White Hall
Cornell University
Ithaca, NY 14853
USA



Mathematics Subjects Classifications (1991): 16-01, 13A20, 20Cxx

Library of Congress Cataloging-in-Publication Data
Farb. Benson.
Noncommutative algebra 1 Benson Farb, R. Keith Dennis.
p. cm. -- (Graduate texts in mathematics: 144)
Includes bibliographical references and index.
ISBN 978-1-4612-6936-6 ISBN 978-1-4612-0889-1 (eBook)
DOI 10.1007/978-1-4612-0889-1
I. Noncommutative algebras. I. Dennis, R.K. (R. Keith). 1944-
II. Title. III. Series
QA251.4.F37 1993
512' .24--dc20 93-17487

Printed on acid-free paper.



Production managed by jim Harbison; manufacturing supervised by Vincent Scelta.
Photocomposed pages prepared from the authors' LaTeX file.

9 8 7 6 5 4 3 2 1

ISBN 978-1-4612-6936-6

Dedicated to the memory of
Paul Farb
and
Eleanor York

# Preface

## About This Book

This book is meant to be used by beginning graduate students. It covers basic material needed by any student of algebra, and is essential to those specializing in ring theory, homological algebra, representation theory and K-theory, among others. It will also be of interest to students of algebraic topology, functional analysis, differential geometry and number theory.

Our approach is more homological than ring-theoretic, as this leads the student more quickly to many important areas of mathematics. This approach is also, we believe, cleaner and easier to understand. However, the more classical, ring-theoretic approach, as well as modern extensions, are also presented via several exercises and sections in Chapter Five. We have tried not to leave any gaps on the paths to proving the main theorems - at most we ask the reader to fill in details for some of the sideline results; indeed this can be a fruitful way of solidifying one's understanding.

The exercises in this book are meant to provide concrete examples to concepts introduced in the text, to introduce related material, and to point the way to further areas of study. Our philosophy is that the best way to learn is to do; accordingly, the reader should try to work most of the exercises (or should at least read through all of the exercises). It should be noted, however, that most of the "standard" material is contained in the text proper. The problems vary in difficulty from routine computation to proofs of well-known theorems. For the more difficult problems, extensive hints are (almost always) provided.

The core of the book (Chapters Zero through Four) contains material which is appropriate for a one semester graduate course, and in fact there should be enough time left to do a few of the selected topics. Another option is to use this book as a starting point for a more specialized course on representation theory, ring theory, or the Brauer group. This book is also suitable for self study.

Chapter Zero covers some of the background material which will be used throughout the book. We cover this material quickly, but provide references which contain further elaboration of the details. This chapter should never actually be read straight through; the reader should perhaps skim it quickly

before beginning with the real meat of the book, and refer back to Chapter Zero as needed.

Chapter One covers the basics of semisimple modules and rings, including the Wedderburn Structure Theorem. Many equivalent definitions of semisimplicity are given, so that the reader will have a varied supply of tools and viewpoints with which to study such rings. The chapter ends with a structure theorem for simple artinian rings, and some applications are given, although the most important applications of this material come in the selected topics later in the book, most notably in the representation theory of finite groups. Exercises include a guided tour through the well-known theorem of Maschke concerning semisimplicity of group rings, as well as a section on projective and injective modules and their connection with semisimplicity.

Chapter Two is an exposition of the theory of the Jacobson radical. The philosophy behind the radical is explored, as well as its connection with semisimplicity and other areas of algebra. Here we follow the above style, and provide several equivalent definitions of the Jacobson radical, since one can see a creature more clearly by viewing it from a variety of vantage points. The chapter concludes with a discussion of Nakayama's Lemma and its many applications. Exercises include the concepts of nilpotence and nilradical, local rings, and the radical of a module.

Chapter Three develops the theory of central simple algebras. After a discussion of extension of scalars and semisimplicity (with applications to central simple algebras), the extremely important Skolem-Noether and Double-Centralizer Theorems are proven. The power of these theorems and methods is illustrated by two famous, classical theorems : the Wedderburn Theorem on finite division rings and the Frobenius Theorem on the classification of central division algebras over **R**. The exercises include many applications of the Skolem-Noether and Double-Centralizer Theorems, as well as a thorough outline of a proof of the well-known Jacobson-Noether Theorem.

Chapter Four is an introduction to the Brauer group. The Brauer group and relative Brauer group are defined and shown to be groups, and as many examples as possible are given. The general study of $Br(k)$ is reduced to that of studying $Br(K/k)$ for galois extensions $K/k$. This allows a more thorough, concrete study of the Brauer group via factor sets and crossed product algebras. Group cohomology is introduced, and an explicit connection with factor sets is given, culminating in a proof that $Br(K/k)$ is isomorphic to $H^2(Gal(K/k), K^*)$. A complete proof of this extremely important theorem seems to have escaped much of the literature; most authors show only that the above two groups correspond *as sets*. There are exceptions, such as Herstein's classic *Noncommutative Rings*, where an extremely involved computational proof involving idempotents is given. We give a clean, elegant, and easy to understand proof due to Chase. This is the first time this proof appears in an English textbook. The chapter ends

with applications of this homological characterization of the Brauer group, including the fact that $Br(K/k)$ is torsion, and a primary decomposition theorem for central division algebras is given.

Chapter Five introduces the notion of primitive ring, generalizing that of simple ring. The theory of primitive rings is developed along lines parallel to that of simple rings, culminating in Jacobson's Density Theorem, which is the analogue for primitive rings of the Structure Theorem for Simple Artinian Rings. Jacobson's Theorem is used to give another proof of the Structure Theorem for Simple Artinian Rings; indeed this is the classical approach to the subject. The Structure Theorem for Primitive Rings is then proved, and several applications of the above theorems are given in the exercises.

Chapter Six provides a quick introduction to the representation theory of finite groups, with a proof of Burnside's famous $p^a q^b$ theorem as the final goal. The connection between representations of a group and the structure of its group ring is discussed, and then the Wedderburn theory is brought to bear. Characters are introduced and their properties are studied. The Orthogonality Relations for characters are proved, as is their consequence that the number of absolutely irreducible representations of a finite group divide the order of the group. A nice criterion of Burnside for when a group is not simple is shown, and finally all of the above ingredients are brought together to produce a proof of Burnside's theorem.

Chapter Seven is an introduction to the global dimension of a ring. We take the elementary point of view set down by Kaplansky, hence we use projective resoultions and prove Schanuel's Lemma in order to define projective dimension of a module. Global dimension of a ring is defined and its basic properties are studied, all with an eye toward computation. The chapter concludes with a proof of the Hilbert Syzygy Theorem, which computes the global dimension of polynomial rings over fields.

Chapter Eight gives an introduction to the Brauer group of a commutative ring. Azumaya algebras are introduced as generalizations of central simple algebras over a field, and an equivalence relation on Azumaya algebras is introduced which generalizes that in the field case. It is shown that endomorphism algebras over faithfully projective modules are Azumaya. The Brauer group of a commutative ring is defined and shown to be an abelian group under the tensor product. $Br()$ is shown to be a functor from the category of commutative rings and ring homomorphisms to the category of abelian groups and group homomorphisms. Several examples and relations between Brauer groups are then discussed.

The book ends with a list of supplementary problems. These problems are divided into small sections which may be thought of as "mini-projects" for the reader. Some of these sections explore further topics which have already been discussed in the text, while others are concerned with related material and applications.

## About Other Books

Any introduction to noncommutative algebra would most surely lean heavily on I.N. Herstein's classic *Noncommutative Rings*; we are no exception. Herstein's book has helped train several generations of algebraists, including the older author of this book. The reader may want to look at this book for a more classic, ring-theoretic view of things.

The books *Ring Theory* by Rowen and *Associative Rings* by Pierce cover similar material to ours, but each is more exhautive and at a higher level. Hence these texts would be suitable for reading after completing Chapters One through Four of this book; indeed they take one to the forefront of modern research in Ring Theory.

Other books which would be appropriate to read as either a companion or a continuation of this book are included in the references.

## Acknowledgments

Many people have made important contributions to this project. Some parts of this book are based on notes from courses given over the years by Professors K. Brown and R.K. Dennis at Cornell University. Professor D. Webb read the manuscript thoroughly and made numerous useful comments. He worked most of the problems in the book and came up with many new exercises. It is not difficult to see the influence of Brown and Webb on this book - any insightful commentary or particularly clear exposition is most probably due to them. Thanks are also due to Professor G. Bergman, B. Grosso, Professor S. Hermiller, Professor T.Y. Lam and Professor R. Laubenbacher, all of whom read the various parts of the manuscript and made many useful comments and corrections. Thanks to Paul Brown for doing most of the diagrams, and to Professor John Stallings for his computer support. We would also like to thank Professors M. Stillman and S. Sen for using this book as part of their graduate algebra courses at Cornell, and we thank their students for comments and corrections. Several exercises, as well as the clever and enlightening new proof that $Br(K/k)$ is isomorphic to $H^2(G, K^*)$, are due to Professor S. Chase, to whom we wish to express our gratitude.

Benson Farb was supported by a National Science Foundation Graduate Fellowship during the time this work took place. R.Keith Dennis would like to thank S. Gersten, who first taught him algebra, and Benson Farb would like to thank R.Keith Dennis, who first taught him algebra. A special thanks goes from B. Farb to Craig Merow, who first showed him the beauty of mathematics, and pointed out the fact that it is possible to spend one's life thinking about such things. Finally, B. Farb would like to thank R.Keith Dennis for his positive reaction to the idea of this project, and especially for the kindness and hospitality he has shown him over the last few years.

## A Word About Conventions

On occasion we will use the words "category" and "functorial", as they are the proper words to use. We do not, however, formally define these terms in this book, and the reader who doesn't know the definitions may look them up or continue reading without any loss.

When making references to other papers or books, we will write out the full name of the text instead of making a reference to the bibliography at the back of the book. We do this so that the reader may know which book we are refering to without having to look it up in the back. In addition, the complete information on each reference is contained in the bibliography.

# Contents

# Part I

# The Core Course

# 0

# Background Material

This chapter contains some of the background material that will be used throughout this book. The goal of this chapter is to fill in certain small gaps for the reader who already has some familiarity with this background material. This should also indicate how much we assume the reader already knows, and should serve to fix some notation and conventions. Accordingly, explanations will be kept to a minimum; the reader may consult the references given at the end of the book for a thorough introduction to the material. This chapter also contains several exercises, for use both by instructors and readers wishing to make sure they understand the basics. The reader may want to begin by glancing casually through this chapter, leaving a thorough reading of a section for when it is needed.

## Rings: Some Basics

We begin with a rapid review of the definitions and basic properties of rings.

A **ring** $R$ is a set with two binary operations, called addition and multiplication, such that

(1) $R$ is an abelian group under addition.

(2) Multiplication is associative; i.e., $(xy)z = x(yz)$ for all $x, y, z \in R$.

(3) There exists an element $1 \in R$ with $1x = x1 = x$ for all $x \in R$.

(4) The distributive laws hold in $R$ : $x(y+z) = xy + xz$ and $(y+z)x = yx + zx$ for all $x, y, z \in R$.

The element $1 \in R$ is called the **identity**, or **unit element** of the ring $R$. We will always denote the unit element for addition by 0, and the unit element for multiplication by 1. $R$ is a **commutative ring** if $xy = yx$ for all $x, y \in R$. We shall *not* assume that our rings are commutative unless otherwise specified.

**Examples:**

1. $\mathbf{Z}$, the integers, with the usual addition and multiplication, with 0 and 1 as additive and multiplicative unit elements.

2. $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$; the rational numbers, real numbers, and complex numbers, respectively, with operations as in Example 1.

3. The ring $\mathbf{Z}/n\mathbf{Z}$ of integers $\bmod n$, under addition and multiplication $\bmod n$.

4. $R[x]$, the ring of polynomials with coefficients in a ring $R$, is a ring under addition and multiplication of polynomials, with the polynomials 0 and 1 acting as additive and multiplicative unit elements, respectively.

5. The ring $\mathcal{M}_n(R)$ of $n \times n$ matrices with entries in a ring $R$ , under addition and multiplication of matrices, and with the $n \times n$ identity matrix as identity element.

6. The ring $End(M)$ of endomorphisms of an abelian group $M$, under addition and composition of endomorphisms (recall that an endomorphism of $M$ is a homomorphism from $M$ to itself).

7. The ring of continuous real-valued functions on an interval $[a, b]$, under addition and multiplication of functions.

The rings in examples 1,2,3, and 7 are commutative; the rings in examples 4,5 and 6 are generally not ($R[x]$ is commutative if and only if $R$ is commutative). We shall encounter many more examples of rings, many of which will not be commutative.

A **ring homomorphism** is a mapping $f$ from a ring $R$ to a ring $S$ such that

(1) $f(x+y) = f(x) + f(y)$; i.e., $f$ is a homomorphism of abelian groups.

(2) $f(xy) = f(x)f(y)$.
(3) $f(1) = 1$.

In short, $f$ preserves addition, multiplication, and the identity element. For those more familiar with groups than with rings, note that (3) does not follow from (1) and (2). For example, the homomorphism $f : \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ given by $f(x) = (x, 0)$ satisfies (1) and (2), but not (3).

The composition of ring homomorphisms is again a ring homomorphism. An **endomorphism** of a ring is a (ring) homomorphism of the ring into itself. An **isomorphism** of rings is a ring homomorphism $f : R \longrightarrow S$ which is one-to-one and onto; in this case, $R$ and $S$ are said to be **isomorphic** as rings. If $f : R \longrightarrow S$ and $g : S \longrightarrow R$ are ring homomorphisms such that $f \circ g$ and $g \circ f$ are the identity homomorphisms of $S$ and $R$, respectively, then both $f$ and $g$ are ring isomorphisms.

A subset $S$ of a ring $R$ is called a **subring** if $S$ is closed under addition and multiplication and contains the same identity element as $R$. A subset

$I$ of a ring $R$ is called a **left ideal** of $R$ if $I$ is a subgroup of the additive group of $R$ and if $ri \in I$ for all $r \in R, i \in I$; the notions of right ideal and two-sided ideal are similarly defined. We shall always assume, unless otherwise specified, that all ideals are left ideals. An ideal $I$ is said to be a **maximal ideal** of the ring $R$ if $I \neq R$ and if $I \subseteq J \subseteq R$ for some ideal $J$, then $J = I$ or $J = R$.

For a two-sided $I$, the quotient group $R/I$ inherits a natural ring structure given by $(r+I)(s+I) = rs + I$. This ring is called the **quotient ring** of $R$ by $I$. Note that there is a one-to-one, order-preserving correspondence between ideals of $R/I$ and ideals of $R$ containing $I$.

A **zero-divisor** in a ring $R$ is an element $r \in R$ for which $rs = 0$ for some $s \neq 0$. An element $r \in R$ is called a **unit** of $R$, and is said to be **invertible**, if $rs = sr = 1$ for some $s \in R$. Note that the set of invertible elements of a ring $R$ forms a group under multiplication, called the **group of units** of $R$. A ring such that $1 \neq 0$, and such that every nonzero element is invertible, is called a **division ring**. A commutative division ring is called a **field**.

Let $F$ be a field and let $n$ be the smallest integer for which $1 + \cdots + 1 = n \cdot 1 = 0$. We call $n$ the **characteristic** of $F$, denoted $char(F)$, and we let $char(F) = 0$ if no such (finite) $n$ exists. It is easy to show that the characteristic of any field is either 0 or prime. For example, $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$ are fields of characteristic 0. $\mathbf{F}_q$, the field with $q = p^n$ ($p$ prime) elements, is a field of characteristic $p$.

## Modules: Some Basics

Let $R$ be a ring. A **left** $R$**-module** is an abelian group $M$, written additively, on which $R$ acts linearly; that is, there is a map $R \times M \longrightarrow M$, denoted by $(r, m) \longmapsto rm$ for $r \in R, m \in M$, for which

(1) $(r+s)m = rm + sm$

(2) $r(m+n) = rm + rn$

(3) $(rs)m = r(sm)$

(4) $1m = m$

for $r, s \in R$ and $m, n \in M$. Equivalently, $M$ is an abelian group together with a ring homomorphism $\rho : R \longrightarrow End(M)$, where $End(M)$ denotes the ring of group endomorphisms of an abelian group (for those unfamiliar with this notion, see page 13). $\rho$ is called the **structure map**, or a **representation** of the ring $R$. There is a corresponding notion of right module, but, unless otherwise specified, we shall assume all modules are left modules.

**Examples:**

1. An ideal $I$ of a ring $R$ is an $R$-module. In particular, $R$ is an $R$-module.
2. Any vector space over a field $k$ is a $k$-module. A module over a division ring $D$ is sometimes called a vector space over $D$.
3. Any abelian group is a $\mathbf{Z}$-module.
4. The cartesian product $R^n = R \times \cdots \times R$ is an $R$-module in the obvious way. $R^n$ is called the **free module of rank $n$**.
5. The set of $n \times n$ matrices $\mathcal{M}_n(R)$ over a ring $R$ is an $R$-module under addition of matrices. The action of $R$ on $\mathcal{M}_n(R)$ is defined, for $r \in R, B \in \mathcal{M}_n(R)$, to be $r \longmapsto rB$, where $rB$ denotes the matrix whose $i,j$th entry is $r$ times the $i,j$th entry of $B$.

Let $M$ and $N$ be $R$-modules. A mapping $f : M \longrightarrow N$ is an **$R$-module homomorphism** if :

(1) $f(m+n) = f(m) + f(n)$
(2) $f(rm) = rf(m)$

for all $m, n \in M, r \in R$. In this case $f$ is also called **$R$-linear**. Note that the composition of two module homomorphisms is again a module homomorphism. A **(module) endomorphism** is a homomorphism of a module to itself. A module homomorphism $f : M \longrightarrow N$ which is one-to one and onto is called a **(module) isomorphism**, in which case $M$ and $N$ are said to be isomorphic modules.

A subset $N$ of a module $M$ is called a **submodule** of $M$, if $N$ is an (additive) subgroup of $M$ and if $rn \in N$ for all $r \in R, n \in N$. Thus, the $R$-submodules of $R$ are precisely the (left) ideals of $R$. If $f : M \longrightarrow N$ is a homomorphism of $R$-modules, let

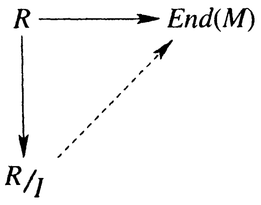
$$\begin{aligned} ker(f) &= \{m \in M : f(m) = 0\} \\ im(f) &= f(M) \end{aligned}$$

be the kernel and the image of $f$. It is easy to check that $ker(f)$ is a submodule of $M$ and $im(f)$ is a submodule of $N$. In particular, for fixed $m \in M$, the kernel of the $R$-module homomorphism $\phi : R \longrightarrow M$ given by $\phi(r) = rm$, is a submodule (i.e., left ideal) of $R$. More explicitly, this kernel is $\{r \in R : rm = 0\}$. This ideal of $R$ is called the **annihilator** of $m$, and is denoted by $ann(m)$. The intersection of the annihilators of each of the elements of $M$ is called the **annihilator of $M$**, and is denoted $ann(M)$; that is

$$ann(M) = \bigcap_{m \in M} ann(m)$$

An $R$-module $M$ is called **faithful** if $ann(M) = 0$. In this case the associated representation $\rho$ is also called a **faithful representation** of $R$.

The abelian group $M/N$ inherits a natural $R$-module structure via $r(m+N) = rm+N$. This $R$-module is called the **quotient module** of $M$ by $N$. Note that there is a one-to-one, order preserving correspondence between submodules of $M/N$ and submodules of $M$ containing $N$. This is sometimes referred to as the Correspondence Theorem for Modules. If $I$ is a two-sided ideal of a ring $R$, and if $M$ is an $R/I$-module, then $M$ is also an $R$-module via $R \longrightarrow R/I \longrightarrow End(M)$. Further, given an $R$-module $M$ which is annihilated by $I$ (i.e., $I \subseteq ann(m)$ for all $m \in M$), there is a unique $R/I$-module structure on $M$ giving rise to the original structure on $M$ :




Thus, there is a one-to-one correspondence between $R/I$-modules and $R$-modules annihilated by $I$.

We shall now discuss certain operations on rings and modules which will be useful later in the text. If $M$ is an $R$-module and $N \subseteq M, I \subseteq R$ are additive subgroups, then $IN$ is defined to be the additive subgroup generated by $\{rn : r \in I, n \in N\}$; that is, $IN = \{\sum_{i=1}^{m} r_i n_i : m \in \mathbf{N}, r_i \in I, n_i \in N\}$. Note that if $N$ is a submodule of $M$, then $IN \subseteq N$, and if $I$ is a left ideal of $R$, then $IN$ is a submodule. In particular, if $M = R$, then $IN$ is a product of ideals. The following formulas hold for $I, I_1, I_2 \subseteq R$ and $N, N_1, N_2 \subseteq M$ :

$$\text{Associative Law}: \quad I_1(I_2N) = (I_1I_2)N$$

Both sides are the additive subgroup generated by products $r_1r_2n$.

$$\text{Distributive Laws}: \quad \begin{aligned} (I_1+I_2)N &= I_1N + I_2N \\ I(N_1+N_2) &= IN_1 + IN_2 \end{aligned}$$

If $M$ is an $R$-module and $m \in M$, then $Rm$ is a submodule of $M$ and is said to be the **cyclic submodule** of $M$ generated by $m$.

## Zorn's Lemma

Zorn's Lemma is used frequently in ring theory. Here we include one typical application.

A **partially ordered set** is a set $S$, together with a relation $\leq$, which satisifies

| | |
|---|---|
| $a \leq a$ | (reflexive) |
| $a \leq b$ and $b \leq c$ implies $a \leq c$ | (transitive) |
| $a \leq b$ and $b \leq a$ implies $a = b$ | (anti-symmetric) |

for all $a, b, c \in S$. A subset $T \subseteq S$ is called a **chain** if either $a \leq b$ or $b \leq a$ for all $a, b \in T$. An **upper bound** for a chain $T$ in $S$ is an element $c \in S$ such that $a \leq c$ for all $a \in T$. An element $c \in S$ is called a **maximal element** of $S$ if $a \in S$ and $c \leq a$ implies $c = a$. We now state

**Lemma 0.1 (Zorn's Lemma)** *Let $S$ be a partially ordered set. If every chain $T$ of $S$ has an upper bound in $S$, then $S$ has at least one maximal element.*

Zorn's Lemma is logically equivalent both to the Axiom of Choice and to the Well-ordering Principle. For proofs of these equivalences, see Halmos, *Naive Set Theory.* For those who worry about using the Axiom of Choice (and thus Zorn's Lemma), we shall always point out where Zorn's Lemma is used.

We conclude this section with a typical application of Zorn's Lemma.

**Proposition 0.2** *Let $R \neq 0$ be a ring (with 1). Then $R$ has a maximal left ideal.*

**Proof:** Let $\mathcal{S}$ be the set of proper (i.e., $\neq R$) left ideals of $R$, partially ordered by inclusion. If $\{I_\alpha\}$ is a chain of ideals in $R$, then for all $\alpha$ and $\beta$, either $I_\alpha \subseteq I_\beta$ or $I_\beta \subseteq I_\alpha$. It is now easy to check that $I = \bigcup_\alpha I_\alpha$ is an ideal of $R$, and that $1 \notin I$ since $1 \notin I_\alpha$ for any $\alpha$. Thus $I \in \mathcal{S}$ and $I$ is an upper bound for the chain. Hence $\mathcal{S}$ contains a maximal element. □

## Products

Let $R_1$ and $R_2$ be rings. Then the cartesian product $R_1 \times R_2 = \{(r_1, r_2) : r_1 \in R_1, r_2 \in R_2\}$ is a ring if addition and multiplication are taken coordinatewise. The ring $R_1 \times R_2$ is called the **product** of the rings $R_1$ and $R_2$. There are natural ring homomorphisms $p_i : R_1 \times R_2 \longrightarrow R_i$ given by projection onto the $i$th coordinate, $i = 1, 2$. There is also a one-to-one map

$$R_1 \longrightarrow R_1 \times R_2$$

$$(r_1, r_2) \longmapsto (r_1, 0).$$

The same holds true for $R_2$. This is not, however, a ring homomorphism, since it does not preserve identity elements. Thus $R_1$ and $R_2$ sit inside $R_1 \times R_2$ as two-sided ideals, but not as subrings. Given rings $R_1, \ldots, R_n$, we may form the product $\prod_{i=1}^{n} R_i$ as was done in the case $n = 2$. The product of $n$ copies of a ring $R$ is denoted by $R^n$.

Given any index set $I$ (possibly infinite), and a family of modules $\{M_i\}_{i \in I}$, we may, by the same technique as above, construct the product $\prod_{i \in I} M_i$ of these modules. An element of $\prod_{i \in I} M_i$ consists of a family of elements $\{m_i \in M_i\}$, which we think of as '$I$-tuples'. The submodule of $\prod_{i \in I} M_i$ consisting of those elements $\{m_i \in M_i\}$ for which all but finitely many of the $m_i$ are zero, is called the **direct sum** of the modules $\{M_i\}_{i \in I}$, and is denoted by $\bigoplus_{i \in I} M_i$. Note that for finite families of modules, the direct sum and the product are the same. If $M'$ is a submodule of $M$, and if $M \approx M' \bigoplus M''$ for some module $M''$, then $M'$ is said to be a **direct summand** of $M$.

Given a subset $S$ of an $R$-module $M$, a **linear combination** of elements of $S$ is a finite sum $\sum r_i s_i$, where each $r_i \in R$ and each $s_i \in S$. We will always write linear combinations so that the $s_i$ are distinct, which is always possible by combining terms. The elements $r_i$ are called the **coefficients** of the linear combination. The set of all linear combinations of elements of $S$ is the unique smallest submodule of $M$ containing $S$, and is called the **submodule generated by** $S$ . The elements of $S$ are then said to generate the submodule. A module is said to be **finitely generated** if it contains a finite generating set.

A subset $S$ of an $R$-module $M$ is **linearly independent** over $R$ if, for every linear combination $\sum r_i s_i$ which is equal to 0, then $r_i = 0$ for all $i$; informally, there are no "relations" among the elements of $S$. In this case we will also say that the elements of $S$ are linearly independent. A subset is **linearly dependent** over $R$ if it is not linearly independent. A subset $S$ of an $R$-module $M$ forms a **basis for** $M$ **over** $R$ if $S$ generates $M$ and is linearly independent over $R$.

Given a family $\{M_i\}$ of submodules of an $R$-module $M$, the **sum** $\sum M_i$ of the family of submodules is defined to be the submodule generated by the union of the $M_i$; or, equivalently, $\sum M_i$ is the set of all finite sums $\sum m_i$, $m_i \in M_i$. The sum is a direct sum, and $M$ is isomorphic to the direct sum of the submodules $M_i$, if every element of $M$ can be written uniquely as a finite sum $\sum m_i$, $m_i \in M_i$.

If a set of elements $\{m_1, \ldots, m_n\}$ forms a basis for the $R$-module $M$, then it is easy to check that $M$ is isomorphic to $R^n$, and in this case $M$ is said to be a **free module of rank** $n$. In the case when $R$ is a field

or a division algebra we call $n$ the **dimension** of $M$ over $R$, denoted by $dim_R(M)$, or simply $dim(M)$ , when there is no confusion about which ring we are talking about.

# Algebras

It turns out that many important examples of modules have an additional multiplicative structure which makes them rings as well, and the module and ring structures are compatible in some sense. Examples to keep in mind are matrix rings, polynomial rings, group rings, and the quaternions (which we shall introduce in this section). The notion of an algebra ties the ring and module structures together, and is one of the basic objects of study in mathematics, particularly in this book. Although we give the definition of an algebra over a commutative ring $k$, we shall only be interested in the case when $k$ is a field.

**Definition:** An (associative) **algebra** over a commutative ring $R$ is a ring $A$ which is also a module over $R$, such that the ring and module multiplication are compatible in the following way :

$$x(ab) = (xa)b = a(xb) \qquad \text{for all } x \in R, a, b \in A.$$

$A$ is also called a ***R*-algebra**. When $R$ is a field, a basis for $A$ as a module over $R$ is said to be a basis for the algebra $A$, and $A$ is said to be a **finite dimensional** $R$-algebra, if $A$ is finite dimensional as a module over $R$ (i.e., if $A$ has a finite basis over $R$). The algebra $A$ is a **commutative algebra** if $A$ is a commutative ring.

**Examples:**

1. Any ring is an algebra over $\mathbf{Z}$.
2. $\mathbf{C}$ is a two-dimensional algebra over $\mathbf{R}$, with basis $\{1, i\}$.
3. The set of $n \times n$ matrices $\mathcal{M}_n(k)$ over a field $k$ is a $k$-algebra of dimension $n^2$. A basis for this algebra consists of the matrices $\{e_{ij}\}, 1 \leq i, j \leq n$, where $e_{ij}$ denotes the matrix with 1 in the $i, j$ position and zeros elsewhere.
4. The ring $R[x]$ is an algebra over the ring $R$, with basis $1, x, x^2, \ldots$ as a (free) $R$-module, and with multiplication of polynomials as the algebra multiplication.
5. The ring $R[[x]]$ of formal power series $\sum_{i=0}^{\infty} r_i x^i$ with coefficients $r_i \in R$ is an $R$-algebra with the obvious multiplication. Similarly, the ring $R[x, x^{-1}]$ of Laurent series is an $R$-algebra.

6. Let $R$ be a ring and let $G$ be a group. The **group ring $R[G]$** consists of the free $R$-module on the set $G$; elements are usually written as $\sum_{g\in G} r_g g$, where $r_g \in R$, and only finitely many $r_g$ are non-zero. Multiplication is defined by extending $(rg)(sh) = (rs)(gh)$ to all of $R[G]$ by the distributive law. Check that this makes $R[G]$ into a ring. Note that $R = R\cdot 1$ is naturally a subring of $R[G]$. For a commutative ring $R$ and a group $G$, the group ring $R[G]$ is an algebra over $R$. $R[G]$ is often called a **group algebra**.

Let $A$ and $B$ be $R$-algebras. A map $f : A \longrightarrow B$ is an **$R$-algebra homomorphism** if $f$ is a homomorphism of $R$-modules which is a homomorphism of rings as well; that is

(1) $f(a+b) = f(a) + f(b)$
(2) $f(xa) = xf(a)$
(3) $f(ab) = f(a)f(b)$
(4) $f(1) = 1$

for all $a, b \in A, x \in R$. An $R$-algebra homomorphism which is one-to-one and onto is called a **$R$-algebra isomorphism** , in which case the algebras are said to be isomorphic algebras. A subset $S$ of an algebra $A$ is called a **subalgebra** if $S$ is both a subring and a submodule of $A$.

We end this section with the construction of a basic, important example of an algebra. Recall that we can think of $\mathbf{C}$ as a two-dimensional algebra with basis $\{1, i\}$ over $\mathbf{R}$. We shall now construct a four-dimensional algebra, the quaternions, with basis $\{1, i, j, k\}$ over $\mathbf{R}$. The quaternions will give an example of a division ring for which multiplication is not commutative. Later in this book we shall see why the number four is special, and why the quaternions and its generalizations play such an important role in the theory of noncommutative algebra.

**Definition:** The (real) **Quaternions**, denoted $\mathbf{H}$ (in honor of its discoverer Hamilton), is the four-dimensional vector space over $\mathbf{R}$ with basis denoted by $\{1, i, j, k\}$, and multiplication defined so that 1 is the multiplicative identity element and

$$\begin{aligned} i &= j = k = -1 \\ ij &= -ji = k \\ jk &= -kj = i \\ ik &= -ki = -j. \end{aligned}$$

These equations (in fact the first two) completely determine how basis elements are multiplied, and thus how any elements of the algebra are multiplied. Every element $q = a + bi + cj + dk \in \mathbf{H}$ has a **quaternion conjugate** $\overline{q} = a - bi - cj - dk$. It is easy to check that $(\overline{q})(\overline{q}) = \overline{q\,q}$ and that $q\overline{q} = \overline{q}q = a + b + c + d$ . This real number is denoted by $|q|$ .

If $q \neq 0$ then $q$ has multiplicative inverse $q^{-1} = \bar{q}/|q|^2$, which shows that **H** is a division algebra. See the exercises for more on the quaternions.

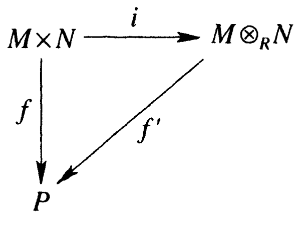
## Tensor Product of Modules Over a Commutative Ring

This section reviews basic properties of the tensor product of modules over a commutative ring. Throughout this section we will assume that $R$ is a commutative ring.

Let $M, N$, and $P$ be $R$-modules. A map $f : M \times N \longrightarrow P$ is said to be an **$R$-bilinear map**, or simply a bilinear map, if $f$ is $R$-linear in each variable when the other variable is fixed; that is, the mappings $x \longmapsto f(x, y_0)$ and $y \longmapsto f(x_0, y)$ are $R$-linear for each fixed $x_0 \in M, y_0 \in N$. The idea of the tensor product is to convert bilinear maps into linear maps (i.e., homomorphisms), which are much easier to work with.

Let $M$ and $N$ be modules over a commutative ring $R$. The **tensor product of $M$ and $N$ (over $R$)** , denoted by $M \otimes_R N$ , can be characterized by the following universal property, which formalizes the idea of "converting" bilinear maps into linear maps :

**Theorem 0.3 (Universal Property of Tensor Product)** *Let $M$ and $N$ be modules over a commutative ring $R$. Then there exists an $R$-module $M \otimes_R N$ and a bilinear map $i : M \times N \longrightarrow M \otimes_R N$ which satisfy the following universal property : Given any $R$-module $P$ and any bilinear map $f : M \times N \longrightarrow P$, there exists a unique linear mapping $f' : M \otimes_R N \longrightarrow P$ so that $f = f' \circ i$; that is, there exists a unique homomorphism $f'$ so that the following diagram commutes*




*Moreover, if there exists an $R$-module $S$ and a bilinear map $j : M \times N \longrightarrow S$ satisfying the above property, then there is an isomorphism $g : M \otimes_R N \longrightarrow S$ with $j = g \circ i$; that is, the tensor product is unique up to isomorphism.*

**Proof:**

Uniqueness : Apply the universal mapping property of $M \otimes_R N$ to $j : M \times N \longrightarrow S$ to get a map $g : M \otimes_R N \longrightarrow S$ with $j = g \circ i$. Similarly,

applying the universal mapping property of $S$ to $i : M \times N \longrightarrow M \otimes_R N$ gives a map $g' : S \longrightarrow M \otimes_R N$ with $i = g' \circ j$. Thus $g \circ g'$ and $g' \circ g$ must be the identity, and so both $g$ and $g'$ are isomorphisms.

Existence : Let $T$ denote the free module generated by the pairs $\{(m, n) : m \in M, n \in N\}$. Thus every element of $T$ can be written as a linear combination $\sum_{i=1}^{n} r_i(m_i, n_i)$ for $r_i \in R$, $(m_i, n_i) \in M \times N$.

Let $V$ denote the submodule of $T$ generated by elements of the following form:

$$\begin{gathered}(m + m', n) - (m, n) - (m', n)\\ (m, n + n') - (m, n) - (m, n')\\ (rm, n) - r(m, n)\\ (m, rn) - r(m, n)\end{gathered}$$

for $m, m' \in M, n, n' \in N, r \in R$. Let $M \otimes_R N$ be the quotient module $T/V$. For each basis element $(m, n)$ of $M \times N$, let $m \otimes n$ denote its image under the quotient map $T \longrightarrow T/V = M \otimes_R N$. Then $M \otimes_R N$ is generated by elements of the form $m \otimes n$. Now define $i : M \times N \longrightarrow M \otimes_R N$ by $i(m, n) = m \otimes n$. It is easy to check from the definitions that $i$ is bilinear.

It remains to check that $M \otimes_R N$ satifies the universal mapping property. To this end, let an $R$-module $P$ and a bilinear map $f : M \times N \longrightarrow P$ be given. We may extend $f$ by linearity to a map $f : T \longrightarrow P$ since $T$ is free with the set $M \times N$ as basis. Since $f$ is bilinear, this implies that $f(V) = 0$, so that there is a well-defined homomorphism $f' : T/V \longrightarrow P$ such that $f'(m \otimes n) = f(m, n)$, and we are done. □

The above proof shows that if $\{u_i\}_{i=1}^{n}$ and $\{v_j\}_{j=1}^{m}$ are generating sets for $M$ and $N$, respectively, then $\{u_i \otimes v_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ is a generating set for $M \otimes_R N$. In particular, if both $M$ and $N$ are finitely generated, then so is $M \otimes_R N$; and, in fact, $dim_R(M \otimes_R N) = dim_R(M) \cdot dim_R(N)$.

Given $R$-modules $M_1, \ldots, M_n$ and an $R$-module $P$, a **multilinear map** (or **$n$-linear map**) is a map $f : M_1 \times \cdots \times M_n \longrightarrow P$ which is $R$-linear in each variable when the other variables are held fixed. The same proof as above gives a construction of the tensor product $M_1 \otimes_R \cdots \otimes_R M_n$ which satisfies the same universal property with respect to multilinear maps. We leave the details as an exercise for the reader.

# Endomorphism Rings

Let $M$ be an abelian group, written additively. Let $End(M)$ denote the set of endomorphisms (i.e., group homomorphisms of $M$ into itself; in particular, every endomorphism takes 0 to 0). If $\phi$ and $\psi$ are endomorphisms of $M$, then $\phi \circ \psi$ is also an endomorphism of $M$, so we may define a multiplication in $End(M)$ via

$$\phi\psi(m) = \phi(\psi(m)) \qquad \text{for } m \in M.$$

The identity endomorphism $1(m) = m$ clearly acts as a multiplicative identity. We may also define an addition in $End(M)$ via

$$(\phi + \psi)(m) = \phi(m) + \psi(m) \qquad \text{for } m \in M.$$

It is trivial to verify that $\phi+\psi \in End(M)$, and that $End(M)$ is an abelian group under this addition, with the endomorphism $0(m) = 0$ acting as the additive identity element. Finally, it is easy to check that, under these operations of addition and multiplication of endomorphisms, $End(M)$ is a ring.

More generally let $M$ and $N$ be $R$-modules, and let $Hom_R(M, N)$ be the set of $R$-module homomorphisms from $M$ to $N$. Then, just as above, we see that $Hom_R(M, N)$ is an abelian group under addition of homomorphisms, with the zero homomorphism acting as identity. We denote $Hom_R(M, M)$ by $End_R(M)$. As above, we see that $End_R(M)$ is a ring, called the **endomorphism ring** of the $R$-module $M$. A **ring of endomorphisms** of $M$ is a subring of $End_R(M)$.

Notice that $End_R(M)$ is also an $R$-module via

$$(r\phi)(m) = r \cdot \phi(m) \qquad r \in R, \phi \in End_R(M), m \in M.$$

If $R$ is a commutative ring, the $R$-module multiplication in $End_R(M)$ is compatible with the ring multiplication of $End_R(M)$. Thus, in this case, $End_R(M)$ is an $R$-algebra, and is called the **endomorphism algebra** of the $R$-module $M$. If $M$ is a free $R$-module of rank $n$, then it is not difficult to see that $End_R(M)$ is isomorphic to the algebra $\mathcal{M}_n(R)$.

## Field Extensions: Some Basics

Let $k$ be a field. A **field extension** of $k$ is a field $K$ with $k \subseteq K$, and is denoted by $\boldsymbol{K/k}$. The smallest field containing $k$ and $r_1, \dots, r_n$ is denoted by $k(r_1, \dots, r_n)$. Given a field extension $K/k$, it is useful to consider $K$ as a vector space over $k$; the abelian group structure is that of $K$, and, for $r \in k, v \in K$, $rv$ is just the the product of $r$ and $v$ in $K$. In fact, since there is actually a multiplication in $K$, and since all operations in sight are commutative, we see that $K$ is an algebra over $k$. The dimension of $K$ as a vector space over $k$ is called the **degree** of the extension $K/k$, and is denoted by $\boldsymbol{[K : k]}$. The extension $K/k$ is called a **finite extension** if $[K : k] < \infty$.

Most of the time we shall be concerned with finite extensions $K/k$. Let $0 \neq u \in K$ for such an extension. Since $K$ is finite dimensional as a vector

space over $k$, the set $\{1, u, u^2, \ldots, u^n\}$ is linearly dependent for some $n$; that is, $c_n u^n + c_{n-1}u^{n-1} + \cdots + c_1 u + c_0 = 0$ for some constants $c_i \in k$. Thus $u$ satisfies the polynomial $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, and $f(x) \in k[x]$. Let $I = \{g(x) \in k[x] : g(u) = 0\}$. Clearly $I$ is an additive subgroup of $k[x]$, and $hg(0) = h(0)g(0) = 0$ for all $h(x) \in k[x], g(x) \in I$, so that $I$ is an ideal. Since $k$ is a field, every ideal in $k[x]$ is principal (see, e.g., Jacobson, *Basic Algebra I*). Since $I$ contains $f(x) \neq 0$, $I$ is not the zero ideal, and so there exists a polynomial $g(x) \in k[x]$ which generates $I$; that is, $g(x)$ divides every polynomial which $u$ satisfies. Clearly we may take $g(x)$ to be a monic polynomial, and then it is easy to see that $g(x)$ is the unique monic polynomial of least degree satisfying $g(u) = 0$. $g(x)$ is called the **minimal polynomial of $u$ over $k$.**

A polynomial is said to be **separable** if it has distinct roots in an algebraic closure. An element $u \in K$ is said to be a **separable element** over $k$ if its minimal polynomial over $k$ is a separable polynomial. A (finite) field extension $K/k$ is said to be a **separable extension** if every element of $K$ is separable over $k$. Note that if $char(k) = 0$, then every (finite) extension of $k$ is separable (see Exercise 35).

A field $L \supseteq k$ is said to be a **splitting field over** $k$ for the polynomial $f(x) \in k[x]$ if $f(x)$ factors as a product of linear factors $f(x) = (x - r_1)\cdots(x - r_n)$ in $L[x]$, and if $L = k(r_1, \ldots, r_n)$. Thus $L$ is a splitting field over $k$ for $f(x)$ if and only if $L$ is the smallest field containing $k$ which contains every root of $f(x)$. A (finite) field extension $K/k$ is called **normal** if every irreducible polynomial in $k[x]$ which has a root in $K$ is a product of linear factors in $K[x]$. Thus the extension $K/k$ is normal if and only if $K$ contains a splitting field for the minimal polynomial of every element of $K$. An extension which is both normal and separable is called a **galois extension.**

Let $K/k$ be a field extension. The set of automorphisms of $K$ which are the identity when restricted to $k$ forms a group under composition of functions. This group is called the **galois group** of the extension $K/k$, and is denoted by $Gal(K/k)$. The Fundamental Theorem of Galois Theory asserts, among other things, that for a galois extension $K/k$, the order of $Gal(K/k)$ is equal to $[K : k]$.

Now suppose $L \supseteq K \supseteq k$ are fields. Then there are three vector spaces in sight; namely $L$ over $K$, $L$ over $k$, and $K$ over $k$. The next result relates the dimensions of these vector spaces, and will be used quite frequently.

**Proposition 0.4** *Let $L \supseteq K \supseteq k$ be fields. Then $[L : k]$ is finite if and only if both $[L : K]$ and $[K : k]$ are finite, and in this case*

$$[L : k] = [L : K][K : k].$$

**Proof:** Suppose $\{u_1, \ldots, u_n\}$ is a basis for $L$ over $K$ and $\{v_1, \ldots, v_m\}$ is a basis for $K$ over $k$. We claim that $\{u_i v_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis for $L$ over $k$:

$\{u_iv_j\}$ span $L/k$: Let $x \in L$ be given. Then $x = \sum_{i=1}^{n} c_i u_i$ for some $c_i \in K$. But $c_i \in K$ implies that $c_i = \sum_{j=1}^{m} d_{ij} v_j$ for some $d_{ij} \in k$. Hence $x = \sum_{i,j} d_{ij} u_i v_j$.

$\{u_iv_j\}$ is independent over $k$: Suppose $\sum d_{ij} u_i v_j = 0$ for some $d_{ij} \in k$. Then $\sum_i (\sum_j d_{ij} v_j) u_i = 0$, and so $\sum_j d_{ij} v_j = 0$ for each $i$, since $\{u_i\}$ is a basis. But $\{v_j\}$ is also a basis, and so $d_{ij} = 0$ for all $j$ and for each $i$.

Now if $[L : k]$ is finite, then $[K : k]$ is finite since $K$ is a $k$-subspace of $L$, and $[L : K]$ is finite since the finite basis for $L$ over $k$ will clearly span $L$ over $K$. Conversely, if both $[L : K]$ and $[K : k]$ are finite, then the above shows that $[L : k]$ is finite and that $[L : k] = [L : K][K : k]$. □

# Exercises

The exercises in this chapter are not meant to be a complete set of exercises for a basic course on rings, fields, and modules; rather, they are meant to help the reader polish old skills. In addition, these exercises provide some basic facts which will be used throughout the text.

## Elementary Exercises on Rings and Modules

1. Let $I_1, \ldots, I_n$ be two-sided ideals of a ring $R$ such that $I_i + I_j = R$ for all $i \neq j$. Prove the following:

   (a) $I_i + \bigcap_{j \neq i} I_j = R$ for all $i$.

   (b) **(Chinese Remainder Theorem):** Given elements $x_1, \ldots, x_n$ of $R$, there exists $x \in R$ such that $x \equiv x_i (mod\ I_i)$ for all $i$.

   (c) Show that there is an isomorphism of rings

   $$\phi : R/I_1 \cap \cdots \cap I_n \longrightarrow (R/I_1) \times \cdots \times (R/I_n)$$

   such that $\phi(x + (I_1 \cap \cdots \cap I_n)) = (x + (I_1), \ldots, x + (I_n))$ for all $x \in R$.

2. Show that every finitely generated module has a maximal (proper) submodule. Is this true for modules that are not finitely generated?

3. Show that every module is isomorphic to a quotient module of a free module.

4. Let $R$ be a commutative ring, and let $M$ be a free $R$-module of rank $n$. Prove that the algebras $End_R(M)$ and $\mathcal{M}_n(R)$ are isomorphic.

**Products and Sums**

5. Let $R_1$ and $R_2$ be rings. Show that any (left,right,two-sided) ideal in $R_1 \times R_2$ is of the form $L_1 \times L_2$, where $L_i$ is a (left,right,two-sided respectively) ideal of $R_i$, $i = 1, 2$.

6. If $R_1$ and $R_2$ are rings, show that there is a one-to-one correspondence between $R_1 \times R_2$-modules $M$ and pairs of modules $(M_1, M_2)$ where each $M_i$ is an $R_i$-module, $i = 1, 2$. Generalize to the case of arbitrary products.

7. Let $R_1$ and $R_2$ be rings. Thinking of $R_1$ as $R_1 \times 0$ sitting inside $R = R_1 \times R_2$, check that $R_1$ is a two-sided ideal but not a subring (similarly for $R_2$). Now show that $R_1 \not\approx R_2$ as $R_1 \times R_2$-modules, even if $R_1 \approx R_2$ as rings. Show that there is in fact no non-trivial $R$-homomorphism from $R_1$ to $R_2$. Generalize to the case of arbitrary products.

8. Let $M = \bigoplus_{i \in I} M_i$ and let $N$ be an arbitrary $R$-module. Prove that a homomorphism from $M$ to $N$ is uniquely determined by its restrictions to the $M_i$ and that these restrictions can be arbitrary. This can be phrased as follows : There is an isomorphism

$$Hom(\bigoplus_i M_i, N) \approx \prod_i Hom(M_i, N).$$

9. Show that there is an isomorphism

$$Hom(N, \prod_i M_i) \approx \prod_i Hom(N, M_i).$$

10. If $E_1, \ldots, E_n, F_1, \ldots, F_m$ are any $R$-modules and $\phi: E_1 \oplus \cdots \oplus E_n \longrightarrow F_1 \oplus \cdots \oplus F_m$ is a $R$-module homomorphism, show that $\phi$ can be represented by a unique matrix

$$M(\phi) = \begin{bmatrix} \phi_{11} & \cdots & \phi_{1n} \\ \vdots & & \vdots \\ \phi_{m1} & \cdots & \phi_{mn} \end{bmatrix}$$

where $\phi_{ij} \in Hom_R(E_j, F_i)$, in the sense that, if one represents an element $x = x_1 + \cdots + x_n \in E_1 \oplus \cdots \oplus E_n$ as a column vector $\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$, and one represents elements of $F_1 \oplus \cdots \oplus F_m$ similarly, then

$$\phi(x) = \begin{bmatrix} \sum_{i=1}^n \phi_{1i}(x_i) \\ \vdots \\ \sum_{i=1}^n \phi_{mi}(x_i) \end{bmatrix}$$

that is, $\phi$ is given by "matrix multiplication". Further, check that composition of maps corresponds to matrix multiplication. This exercise generalizes Proposition 1.7. [Hint: The module $E_1 \oplus \cdots \oplus E_n$ is equipped with inclusions $i_k : E_k \longrightarrow E_1 \oplus \cdots \oplus E_n$ and (onto) projections $\pi_k : E_1 \oplus \cdots \oplus E_n \longrightarrow E_k$.]

**Idempotents**

11. (a) An element $e$ of a ring $R$ is said to be an **idempotent** if $e^2 = e$. An element $e$ is **central in** $R$ if $er = re$ for all $r \in R$. Let $e$ be a central idempotent of $R$, and let $R_1 = eR$ and $R_2 = (1-e)R$. Check that these subsets of $R$ are two-sided ideals of $R$ which are in fact rings. What are the identity elements of $R_1$ and $R_2$ as rings? Show that every element of $R$ can be written uniquely as a sum of an element of $R_1$ and an element of $R_2$. Conclude that $R \approx R_1 \times R_2$ as rings.

    (b) What do the ideals of $R$ look like in terms of the ideals of $R_1$ and $R_2$?

12. (a) More generally, let $e_1, \ldots, e_n$ in $R$ be an **orthogonal family of central idempotents**; that is, assume each $e_i, 1 \leq i \leq n$ is a central idempotent and that $e_i e_j = 0$ for $i \neq j$. Further assume that $e_1 + e_2 + \ldots + e_n = 1$. Show that $R \approx R_1 \times R_2 \times \ldots \times R_n$ where $R_i = e_i R$.

    (b) What do modules over $R$ look like?

13. Let $I$ be a two-sided ideal of $R$, and assume that $R = I \oplus J = I \oplus J'$, where $J$ is a left ideal of $R$ and $J'$ is a right ideal of $R$. Prove that there is a *unique* central idempotent such that $I = Re$, and that then $J = R(1-e) = J'$.

**Tensor Products**

14. Let $M, N$, and $P$ be modules over a commutative ring $R$. Prove the following (all tensoring is done over $R$):

    (a) $M \bigotimes N \approx N \bigotimes M$.

    (b) $(M \bigotimes N) \bigotimes P \approx M \bigotimes (N \bigotimes P) \approx M \bigotimes N \bigotimes P$.

    (c) $(M \bigoplus N) \bigotimes P \approx (M \bigotimes P) \bigoplus (N \bigotimes P)$.

    (d) $R \bigotimes M \approx M$.

## Group Rings

15. (a) If $G$ is the trivial group, what is $R[G]$?

(b) If $G$ is a free abelian group on $n$ generators, what is $R[G]$?

(c) Show that $R[G \times H] \approx R[G] \otimes_R R[H] \approx (R[G])[H]$ as rings.

(d) Show that if $G$ acts linearly on a vector space $V$ over a field $k$, then $V$ has a natural $k[G]$-module structure.

16. (a) Let $R, S$ be rings and let $G$ be a group. Let $U(S)$ denote the group of units of $S$ (that is, the (multiplicative) group of elements in $S$ that have multiplicative inverses). Show that there is a one-to-one correspondence between ring homomorphisms $f : R[G] \to S$ and pairs consisting of a ring homomorphism $f_R : R \to S$ and a group homomorphism $f_G : G \to U(S)$ where the images of $f_R$ and $f_G$ commute.

(b) If $f : G \to H$ is a group homomorphism, show that there is a unique ring homomorphism $R[G] \to R[H]$ which is the identity on $R$ and is $f$ when restricted to $G$.

**Remark:** Consider the case when $R$ is a commutative ring and $S$ is an $R$-algebra, so $f_R$ is fixed as the structure map. The "units" functor $U$ is a functor $S \longmapsto U(S)$ from the category of $R$-algebras to the category of groups. The "group-algebra" functor $G \longmapsto R[G]$ is a functor from groups to $R$-algebras. Holding $f_R$ fixed, the proof of part (a) shows the existence of a bijection

$$Hom_{group}(G, U(S)) \longleftrightarrow Hom_{R-algebra}(R[G], S),$$

that is, the group-algebra functor is the *left-adjoint* to the units functor (for terminology, see Rotman's *Homological Algebra*).

17. (a) If $H$ is a finite subgroup of $G$, write $N_H = \sum_{h \in H} h$ (this is the so-called "norm element" of $H$). Show that $N_H \cdot N_H = |H| N_H$. Conclude that if $|H|$ is invertible in $R$, then the element $e_H = N_H / |H|$ is idempotent.

(b) Show that if $H$ is a finite normal subgroup of $G$ and $|H|$ is invertible in $R$, then $e_H$ is a central idempotent of $R[G]$.

18. Let $\mathbf{Q}$ denote the rational numbers and let $S_3$ denote the symmetric group on 3 letters. Note that $S_3$ is generated by the elements $a = (12)$ and $b = (123)$ with $o(a) = 2$ and $o(b) = 3$, $aba = b^{-1}, S_3 \approx \mathbf{Z}_3 \rtimes \mathbf{Z}_2$.

(a) Show that $\mathbf{Q}[\mathbf{Z}_2] \approx \mathbf{Q} \times \mathbf{Q}$. Exhibit the ring homomorphisms explicitly. Exhibit the idempotents explicitly.

(b) The unique surjective homomorphism $S_3 \to \mathbf{Z}_2$ induces a ring surjection $\mathbf{Q}[S_3] \to \mathbf{Q}[\mathbf{Z}_2] \approx \mathbf{Q} \times \mathbf{Q}$. For $B = (b)$, find the images of $e_B$ and $1 - e_B$, where $e_B$ is defined as in problem 17.

(c) Let $\mathcal{M}_2(\mathbf{Q})$ denote the ring of $2 \times 2$ matrices over $\mathbf{Q}$. Let $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. Show that $o(A) = 2, o(B) = 3$ (can you do this without computing?),and $ABA = B^{-1}$. Thus there is a group homomorphism

$$S_3 \to GL_2(\mathbf{Q}) = U(\mathcal{M}_2(\mathbf{Q})).$$

Show that this gives a surjective ring homomorphism $\mathbf{Q}[S_3] \to M_2(\mathbf{Q})$.

(d) Put all of this together and show that $\mathbf{Q}[S_3] \approx \mathbf{Q} \times \mathbf{Q} \times \mathcal{M}_2(\mathbf{Q})$. Explicitly give all of the homomorphisms. Explicitly list the idempotents (in terms of the group ring) which give each factor. In Chapter One we will see that this implies that $\mathbf{Q}[S_3]$ is semisimple.

**Remark:** This example is typical of group representation theory : you'll soon see that any group algebra $\mathbf{Q}[G]$ ($G$ finite) is a direct product of matrix algebras, and this is a good example to keep in mind. The idea is to "enrich structure" by recasting problems from group theory (which is hard) into the theory of algebras (which is rich and well-developed, as we will see in subsequent chapters).

19. Generalizing part (a) of the previous exercise, show that if $p$ is prime then $\mathbf{Q}[\mathbf{Z}_p] \approx \mathbf{Q} \times \mathbf{Q}[\zeta_p]$, where $\zeta_p$ is a primitive $p^{th}$ root of unity.

### Quaternions

20. Check that $\mathbf{H}$ is a division algebra which is not commutative. Find the center of $\mathbf{H}$; i.e., the set of elements $x \in \mathbf{H}$ which commute (multiplicatively) with every element of $\mathbf{H}$. Which elements commute with $i$? with $j$? with $k$?

21. Let $\mathbf{H_Q}$ be the subset of $\mathbf{H}$ consisting of elements with rational coordinates; that is, let $\mathbf{H_Q} = \{a + bi + cj + dk : a, b, c, d \in \mathbf{Q}\}$ . Show that $\mathbf{H_Q}$ is a subring of $\mathbf{H}$, and that $\mathbf{H_Q}$ is a division ring. $\mathbf{H_Q}$ is called the ring of **rational quaternions.**

22. Let $R$ denote the set of matrices of the form $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$ $a, b \in \mathbf{C}$.

    (a) Show that $R$ is a subring of $\mathcal{M}_2(\mathbf{C})$.

(b) Show that the center of $R$ may be identified with the real numbers via a certain set of diagonal matrices.

(c) Show that $R$ is isomorphic, as an $\mathbf{R}$-algebra, to the real quaternions.

23. Show that the real quaternions can be considered as a two-dimensional algebra over $\mathbf{C}$. Explicitly give a basis for $\mathbf{H}$ over $\mathbf{C}$.

24. Think of $\mathbf{R}^4$ as pairs $(r, v)$, where $r$ is a real number and $v$ is a vector in $\mathbf{R}^3$. Define a multiplication on $\mathbf{R}^4$ by

$$(r, v)(r', v') = (rr' - v \cdot v', rv' + r'v + v \times v') \quad r, r' \in \mathbf{R}, v, v' \in \mathbf{R}^3$$

where $\cdot$ and $\times$ denote the standard dot and cross product of vectors in $\mathbf{R}^3$, respectively. Prove that $\mathbf{R}^4$ with this multiplication is an algebra which is isomorphic to the quaternions. Thus, multiplication of quaternions involves the two most basic operations on vectors in three-dimensional euclidean space. Hamilton, the discoverer of the quaternions, had the idea to use the quaternions to study physics. Physicists, however, seem to have found it easier to use the dot and cross product without mention of the quaternions.

## The Opposite Ring

25. If $R$ is a ring, then $R^\circ$ denotes the **opposite ring** (of $R$) : that is, $R^\circ$ has the same additive group as $R$ but multiplication in $R^\circ$ is defined by $r \cdot s = sr$. Check that $R^\circ$ is a ring.

(a) If $k$ is a commutative ring and $G$ is any group, show that $k[G]^\circ \approx k[G]$.

(b) Let $\mathbf{H}$ denote the division algebra of real quaternions. Show that $\mathbf{H}^\circ \approx \mathbf{H}$.

(c) If $R$ is a ring and $\mathcal{M}_n(R)$ denotes the ring of $n \times n$ matrices over $R$, show that $\mathcal{M}_n(R)^\circ \approx \mathcal{M}_n(R^\circ)$.

(d) Exhibit a ring $R$ such that $R^\circ$ is not isomorphic to $R$. Can you give such a ring that is finite? If so, what is the smallest possible number of elements it can have?

(e) Let $R$ be a commutative ring and let $\mathcal{T}_n(R)$ denote the ring of $n \times n$ upper triangular matrices over $R$. Is $\mathcal{T}_n(R)^\circ$ isomorphic to $\mathcal{T}_n(R)$?

26. Show that $End_R(R) \approx R^\circ$.

27. Show that if $e$ is an idempotent of $R$, then $S = eRe$ is a ring with identity element $e$ (note : by definition $eRe = \{ere : r \in R\}$). Find an isomorphism (of rings)

$$\phi : S^\circ \xrightarrow{\approx} End_R(Re).$$

This generalizes the fact that, for any ring $R$, $End_R(R) \approx R^\circ$ (just take $e = 1$).

**Bimodules**

28. Let $R$ and $S$ be rings. An ***R*-*S* -bimodule** is an abelian group $M$ with the structure of both a left $R$-module and a right $S$-module, such that $(rm)s = r(ms)$ for $r \in R, m \in M, s \in S$. For example, any ring $R$ is an $R$-$R$ bimodule under left and right multiplication. If $R$ and $S$ are $k$-algebras, we will say that $M$ is an **$R$-$S$-bimodule relative to $k$** if, in addition to the above, $\lambda m = m\lambda$ for $\lambda \in k$ and $m \in M$. Prove that $R$-$S$ bimodule structures on $M$ relative to $k$ are in one-to-one correspondence with $R \otimes_k S^\circ$-module structures on $M$.

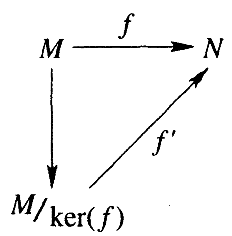
29. Let $e$ and $e'$ be idempotents of a ring $R$, let $S = eRe$ and let $S' = e'Re'$. Note that $S$ and $S'$ are rings with identity elements $e$ and $e'$, respectively. Find $S$-$S'$-bimodule structures on $eRe'$ and $Hom_R(Re, Re')$, and an $S$- $S'$-bimodule isomorphism

$$eRe' \xrightarrow{\approx} Hom_R(Re, Re').$$

Note that, if we now take $e' = 1$, then $eR \approx Hom_R(Re, R)$ as $S$-$R$-bimodules. (cf. Exercise 27).

**Universal Mapping Properties**

30. (a) Show that any $R$-module homomorphism $f : M \longrightarrow N$ "factors through $M/ker(f)$"; that is, show that there is a unique homomorphism $f' : M/ker(f) \longrightarrow N$ so that the following diagram commutes :




Show further that $f'$ is one-to-one. Show that the above holds when $ker(f)$ is replaced by any submodule of $ker(f)$ (of course, the injectivity fails to hold).

(b) Prove a corresponding universal mapping property for homomorphisms of rings.

31. State the results of exercises 8 and 9 in terms of universal mapping properties.

32. Let $M_1, \ldots, M_n$ be modules over a commutative ring $R$. Following the construction given in Theorem 0.3 for the case $n = 2$, construct the tensor product $M_1 \otimes_R \cdots \otimes_R M_n$, and show that it is unique. Prove a universal mapping property for this tensor product which agrees with Theorem 0.3 in the case $n = 2$.

## Elementary Exercises on Field Theory

33. (a) Let $F$ be a field with $char(F) \neq 0$. Show that $char(F)$ is equal to the smallest integer $n$ such that $x + \cdots + x = n \cdot x = 0$ for all $x \in F$.

(b) Show that the characteristic of any field is either 0 or prime. Further, show that any field of characteristic 0 contains **Q** as a subfield.

34. Assuming that **C** is algebraically closed, prove that the only finite field extensions of **R** are **R** and **C**.

35. (a) Let $k$ be a field. Show that a polynomial $f(x) \in k[x]$ has multiple roots (in a splitting field for $f$ over $k$) if and only if $f$ and $f'$ have a common root (in a splitting field), where $f'$ is the polynomial which is the derivative of $f$ as in elementary calculus.

(b) Use part (a) to show that any finite extension of a field of characteristic zero is separable.

36. Show that the field $\mathbf{Q}(\sqrt[3]{2})$ is not a normal extension of **Q**, where $\sqrt[3]{2}$ denotes the real cube root of 2. Recall that $\mathbf{Q}(\sqrt[3]{2})$ denotes the smallest field containing **Q** and $\sqrt[3]{2}$.

## Exact Sequences: Some Basics

A sequence of $R$-modules and $R$-module homomorphisms

$$\cdots \longrightarrow M_{i+1} \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \longrightarrow \cdots$$

is said to be **exact at** $M_i$ if $ker(f_i) = im(f_{i+1})$. The sequence is called an **exact sequence** if it is exact at each $M_i$. A **short exact sequence** is an exact sequence of the form

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0.$$

Note that the sequence is exact at $A$ if and only if $i : A \longrightarrow B$ is one-to-one, and that the sequence is exact at $C$ if and only if $p : B \longrightarrow C$ is onto. Exactness at $B$ means that $C \approx B/i(A)$.

Exact sequences are extremely useful in keeping track of information about maps between modules. They are crucial in the study of algebraic topology, algebraic geometry, and in fact all of algebra. Although exact sequences are not essential for understanding much of this book, they will provide another viewpoint in the study of semisimple rings, the Brauer group and various selected topics.

A short exact sequence

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is said to **split** if there is a homomorphism $h : C \longrightarrow B$ with $g \circ h = id_C$, where $id_C$ denotes the identity endomorphism of $C$.

37. Let $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ be exact. Prove that the following are equivalent:

    (a) The sequence splits.

    (b) The module $f(A)$ is a direct summand in $B$.

    (c) There is a homomorphism $r : B \longrightarrow A$ with $r \circ f = id_A$.

    (d) There is a homomorphism $s : C \longrightarrow B$ such that $g \circ s = id_C$.

38. Let $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ be exact. Show that the sequence splits if $C$ is a free module.

39. (a) Suppose

$$A_1 \xrightarrow{f_1} B_1 \xrightarrow{g_1} C_1 \qquad \text{and} \qquad A_2 \xrightarrow{f_2} B_2 \xrightarrow{g_2} C_2$$

are exact. Show that

$$A_1 \times A_2 \xrightarrow{f_1 \times f_2} B_1 \times B_2 \xrightarrow{g_1 \times g_2} C_1 \times C_2$$

is exact.

    (b) Generalize part (a) to arbitrary direct products.

    (c) Generalize part (a) to arbitrary direct sums.

40. Let $0 \longrightarrow V_1 \longrightarrow \cdots \longrightarrow V_n \longrightarrow 0$ be an exact sequence of finite-dimensional vector spaces over a field. Show that $\sum_{i=1}^{n}(-1)^i dim(V_i) = 0$.

**Length**

A **composition series** for a module $M$ is a chain of submodules $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ which admits no refinement, i.e., $M_i/M_{i-1}$ is simple. We call $n$ the **length** of the composition series. The simple modules $M_i/M_{i-1}$ are called the **composition factors** of the composition series. A given module may have many composition series. These series are related, however, by the following :

**Theorem 0.5 (Jordan-Hölder Theorem)** *If $M$ has a composition series, then any two composition series have the same length and have isomorphic composition factors.*

The proof of this theorem is the same as that for groups. For details see e.g., Jacobson, *Basic Algebra I.* We define the **length** of a module $M$, denoted by $\boldsymbol{l(M)}$, to be the length of a composition series for $M$ (if $M$ doesn't have a composition series, we say that $M$ has **infinite length** ). The length of a module is well-defined by the Jordan-Hölder Theorem. We also note that "length of a module" generalizes the concept of "dimension of a vector space". For example, it is easy to see that if $R$ is an algebra over a field $k$, then any $R$-module $M$ such that $dim_k(M) < \infty$ has finite length.

41. (a) If $M$ is a module of finite length, prove that any submodule and any quotient module of $M$ has finite length.

    (b) Conversely, if $M' \subseteq M$ and $M/M'$ both have finite length, show that $M$ has finite length. Further, show that $l(M) = l(M')+l(M/M')$. Deduce that $l(M') < l(M)$ if $M' \neq M$.

    (c) Prove that a finite direct sum of modules of finite length has finite length and give a formula for the length.

    (d) If $R$ has finite length as a left $R$-module, prove that every finitely generated left $R$-module has finite length (A module $M$ is **finitely generated** if there exists a finite family of elements $m_1, \ldots, m_n$ of $M$ such that $Rm_1 + \cdots + Rm_n = M$).

**Chain Conditions**

We say that a module $M$ satisfies the **ascending chain condition (ACC)** if for every chain $M_1 \subseteq M_2 \subseteq \cdots$ of submodules of $M$, there is an integer $n$ with $M_i = M_n$ for all $i \geq n$. If $M$ satisfies the ACC, we also say that $M$ is **noetherian**.

We say that a module $M$ satisfies the **descending chain condition (DCC)** if for every chain $M_1 \supseteq M_2 \supseteq \cdots$ of submodules of $M$, there is an integer $m$ such that $M_j = M_m$ for all $j \geq m$. If $M$ satisfies the DCC, we say that $M$ is **artinian**.

42. (a) Show that $\mathbf{Z}$ is a noetherian $\mathbf{Z}$-module which is not artinian.

    (b) Let $\mathbf{Z}_{p^\infty}$ denote the submodule of the $\mathbf{Z}$-module $\mathbf{Q}/\mathbf{Z}$ consisting of elements which are annihilated by some power of $p$. Show that $\mathbf{Z}_{p^\infty}$ is an artinian $\mathbf{Z}$-module which is not noetherian.

43. (a) Show that the ACC is equivalent to the "maximal condition" : Every non-empty collection of submodules contains a maximal element (with respect to inclusion).

    (b) Show that the DCC is equivalent to the "minimal condition" : Every non-empty collection of submodules contains a minimal element (with respect to inclusion).

44. Prove that a module is noetherian if and only if every submodule is finitely generated.

45. (a) Prove that submodules and quotients of artinian modules are artinian. Prove the same fact for noetherian modules.

    (b) Let $M'$ be a submodule of $M$. Show that if both $M'$ and $M/M'$ are artinian, then so is $M$. Prove the same fact for noetherian modules.

    In other words, these statements say that given a short exact sequence

    $$0 \to M' \to M \to M'' \to 0,$$

    $M$ is artinian (resp. noetherian) if and only if both $M'$ and $M''$ are artinian (resp. noetherian).

46. Prove that a module has finite length if and only if it is both artinian and noetherian.

**Note:** We shall call a ring $R$ a **(left) noetherian ring** or a **(left) artinian ring** if it has the corresponding property as a left $R$-module. We shall drop the adjective "left" when no confusion will occur.

47. Prove that if $R$ is an artinian ring and $M$ is a finitely generated $R$-module, then $M$ has finite length.

48. Prove that if $M$ is an $R$-module of finite length, then $End_R(M)$ is artinian.

49. This exercise will show that the concepts of left and right artinian (and noetherian) are not the same. Let $K/k$ be a field extension with $[K : k] = \infty$. Let $R$ denote the subset of $\mathcal{M}_2(K)$ consisting of all upper triangular matrices of the form

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$$

with $a, b \in K$ and $c \in k$. Show that $R$ is a subring of $\mathcal{M}_2(K)$, and that $R$ is left artinian and left noetherian, but neither right artinian nor right noetherian.

50. (a) Prove Fitting's Lemma : If $M$ is an artinian module and $f : M \longrightarrow M$ is an injective homomorphism, then $f$ is surjective.

(b) Prove the dual assertion to Fitting's Lemma : If $M$ is a noetherian module and $f : M \longrightarrow M$ is a surjective homomorphism, then $f$ is injective.

(c) Let $G$ be a free abelian group of finite rank, and let $\phi : G \longrightarrow G$ be an epimorphism. Show that $\phi$ is an isomorphism.

# 1

# Semisimple Modules & Rings and the Wedderburn Structure Theorem

This chapter is concerned with looking at part of a structure theory for rings. The idea of any "structure theory" of an object (in this case a ring) is to express that object in terms of simpler, better understood pieces. For example, the Wedderburn Structure Theorem says that any semisimple ring (we'll define this later) is isomorphic to a finite product of matrix rings over division rings, each of which is simple. The theory for semisimple modules is in many ways analogous to the theory of vector spaces over a field, where we can break up vector spaces as sums of certain subspaces.

One common theme in this chapter is the interconnection between the structure of a ring and the structure of modules over that ring. This interplay leads to many deep and useful theorems.

Unless otherwise specified, all ideals will be left ideals and all modules will be left modules.

## Simple Modules

We begin our discussion with modules that are the basic building blocks of other modules.

**Definition:** A non-zero module $M$ is **simple** (or **irreducible**) if it contains no proper non-zero submodule. An $R$-module $M$ is **cyclic with generator** $\boldsymbol{m}$ if $M = Rm$ for some $m \in M$.

If $F$ is a field, then the submodules of a vector space $V$ over $F$ are simply the subspaces of the $V$. The simple $F$-modules are the one-dimensional vector spaces over $F$; thus there is only one isomorphism class of simple $F$-modules. We shall soon see many other examples of simple modules.

**Proposition 1.1** *The following are equivalent for an $R$-module $M$:*
*(1) $M$ is simple.*
*(2) $M$ is cyclic and every non-zero element is a generator.*
*(3) $M \approx R/I$ for some maximal left ideal $I$.*

**Proof:**

(1) implies (2) : If $m \in R, m \neq 0$, then $Rm$ is a non-zero submodule of $M$, hence $Rm = M$.

(2) implies (3) : Let $I$ be the kernel of the surjective module map $\phi : R \longrightarrow Rm$ given by $\phi(r) = rm$ (this kernel is called the **(left) annihilator** of $m$ and is denoted by $ann(m)$). So $I$ is a submodule of $R$, i.e. a left ideal of $R$, and $R/I \approx Rm$. $I$ is maximal : for if not, then there would be a non-generating element of $M$.

(3) implies (1) : If $M'$ is a nonzero submodule of $M \approx R/I$, then by the Correspondence Theorem for Modules (see Chapter 0) we have that there is an ideal $I'$ properly containing $I$. Since $I$ is maximal, $I' = R$, so $M' = M$ and we are done. □

**Note:** It is easy to check that if $R$ is commutative, then the ideal $I$ in (3) is independent of the generator $m \in M$, so $I$ is uniquely determined by $M$; in this case we see that isomorphism classes of simple $R$-modules are in one-to-one correspondence with maximal ideals of $R$ (this is a familiar fact when $R = \mathbf{Z}$).

It is easy to construct many examples of simple modules using (3) above.

**Examples:**

1. The simple $\mathbf{Z}$-modules are $\mathbf{Z}/p\mathbf{Z}$ for $p$ prime.
2. The simple $F[x]$-modules ($F$ a field) are $F[x]/(p)$ for $p$ an irreducible polynomial.
3. Here is a less obvious example : Let $F$ be a field, $V$ an $n$-dimensional vector space over $F$, and let $R = End_F(V)$ ($R$ is often called the "ring of linear operators over $V$"). One sees by choosing a basis for $V$ over $F$ that $R \approx \mathcal{M}_n(F)$, the ring of $n \times n$ matrices with entries in $F$. $V$ is an $R$-module via $f \cdot v = f(v)$; in fact, $V$ is a simple $R$-module: if $v \neq 0$, then $v$ is part of a basis for $V$, so clearly $Rv = V$, hence $V$ satisfies (ii). In fact, we will see that this is the only simple $R$-module, up to isomorphism.

One of the reasons simple modules are so useful and easy to work with is that there are so few homomorphisms between them. Consider a module homomorphism $f : M \longrightarrow N$. Note that $kernel(f)$ and $image(f)$ are submodules of $M$ and $N$, respectively. Thus if $M$ is simple, then $kernel(f)$ is 0 or $M$, and if $N$ is simple then $image(f)$ is 0 or $N$. In particular, if both $M$ and $N$ are simple, then $f$ is either an isomorphism or the zero map. This proves the well-known

**Lemma 1.2 (Schur's Lemma)** *Any homomorphism between simple $R$-modules is either an isomorphism or the zero homomorphism. Therefore $End_R(M)$ is a division ring if $M$ is simple.*

It is also clear that if $M$ and $N$ are simple, and if $M \not\approx N$, then $Hom_R(M,N) = 0$.

**Remarks:**

1. If R is a commutative ring, then

$$End_R(R/I) = End_{R/I}(R/I) \approx R/I$$

since in general we have, for commutative rings $R$, that $End_R(R) \approx R$ via $f \mapsto f(1)$. Note that, in particular, if $M$ is a simple $R$-module, then $M \approx R/I$ for some maximal ideal $I$, and so $End_R(M) \approx End_R(R/I) \approx R/I$, a field. So when $R$ is a commutative ring and $M$ is a simple $R$-module, $End_R(M)$ is not only a division ring, but is in fact a field.

2. If $V$ is a module over a division ring $D$ and $R = End_D(V)$, then $R$ acts on $V$, and the action of $R$ commutes with that of $D$. Thus scalar multiplication induces a homomorphism

$$D \longrightarrow End_R(V)$$

$$d \longmapsto \text{'scalar multiplication by } d\text{'}.$$

In fact, this is an isomorphism :

**Proof:** Since the above homomorphism is clearly injective, we need only show, given $T \in End_R(V)$, that $T$ is multiplication by an element of $D$. Choose $v \neq 0$ in $V$. Given any element $w$ of $V$, it is easy to find an endomorphism of $V$ which carries $v$ to $w$; hence $v$ generates $V$ as an $R$-module. Thus an $R$-module endomorphism $T$ is uniquely determined by what it does to $v$. It therefore suffices to show $Tv = dv$ for some $d \in D$. Now since $v$ is part of a $D$-basis for $V$, there is a projection operator $p \in End_D(V) = R$, where $p$ is the endomorphism that projects any vector in $V$ onto the subspace $Dv$ generated by $v$ (so in particular $p(v) = v$). Then $Tv = T(pv) = p(Tv) \in Dv$ and we're done. □

In fact, the above isomorphism holds for a class of rings more general than division rings, namely semisimple rings. For details see Exercise 18.

3. Suppose that $R$ is an algebra over a field $k$ and $M$ is a simple $R$-module of finite $k$-dimension. Then by Schur's Lemma $End_R(M)$ is a division ring, and, since it lies in $End_k(M)$, is in fact a finite dimensional algebra over $k$ via the natural inclusion

$$k \longrightarrow End_R(M)$$

$$x \longmapsto \text{`multiplication by } x\text{'}.$$

When are all $R$-endomorphisms of M of this form? That is, when is it true that every $R$-endomorphism is just "multiplication by $x$" for some $x \in k$? The following corollary to Lemma 1.2 gives us a partial answer.

**Corollary 1.3** *If $k$ is an algebraically closed field, $R$ an algebra over $k$, and $M$ a simple $R$-module of finite $k$-dimension, then $k \approx End_R(M)$; that is, the only endomorphisms of $M$ are the scalar multiplications by elements of $k$.*

**Proof:** This follows from the fact that the only finite dimensional division algebra over an algebraically closed field is the field itself (see Exercise 1). □

This corollary is the original result proved by Schur, and was stated in the context of group representation theory (with $k = \mathbf{C}$ and $R = \mathbf{C}[G]$). Together, Corollary 1.3 and Schur's Lemma constitute the "orthogonality relations for complex characters" which are so important in representation theory. We will give some indication of the power of these methods in Chapter 6.

## Semisimple Modules

The next level in complexity of modules is to combine simple modules in a simple way, namely with direct sum. The resulting modules are called semisimple, and are one of the basic objects of study in algebra. The philosophy is that semisimple modules behave in many ways like vector spaces over a field, simple modules playing a role analogous to one-dimensional subspaces.

**Definition:** A module $M$ is called **semisimple** if it is a direct sum (not necessarily finite) of simple modules. The Uniqueness Theorem for Semisimple Modules (see Exercise 25) shows that these simple summands are determined (up to isomorphism) by $M$, and so are independent of how we

write the direct sum. The simple modules in the direct sum are called the **(simple) constituents** of $M$.

**Examples:**

1. Any simple module is semisimple.
2. Any vector space $V$ over a division ring is semisimple. If we choose a basis $\{e_i\}_{i\in I}$ for $V$, then the one-dimensional subspaces generated by the $e_i$ are simple modules whose direct sum is $V$.
3. Clearly any direct sum of semisimple modules is semisimple.

We shall see other examples of semisimple modules later.

Recognizing semisimple modules isn't as hard as it looks. For example, $M$ is semisimple if one can write every element of $M$ as a sum of elements of simple submodules.

**Proposition 1.4** *If $M$ is the sum (not necessarily direct) of simple submodules $M_i, i \in I$, then $M$ is semisimple. More precisely, there is a subset $I' \subseteq I$ such that $M = \bigoplus_{i\in I'} M_i$.*

The proof of this proposition is similar to the proof that every vector space has a basis. Recall that a family of submodules $\{M_j\}_{j\in J}$ is called **independent** if $\sum_{j\in J} m_j = 0$ implies that $m_j = 0$ for all $j$ (here $m_j \in M_j$ and $m_j = 0$ for all but finitely many $j$). This is equivalent to saying that $\sum_{j\in J} M_j$ is a direct sum.

**Proof:** Consider the collection $\mathcal{S} = \{J : \{M_j\}_{j\in J}$ is independent$\}$ under the partial order given by inclusion. $\mathcal{S}$ is clearly not empty. Every chain has an upper bound in $\mathcal{S}$ (namely its union) and hence by Zorn's Lemma there exists a maximal element $I'$. Let $M' = \sum_{i\in I'} M_i$. We claim that $M' = M$ : for since each $M_j$ is a simple module, $M' \cap M_j = 0$ or $M' \cap M_j = M_j$. If $M' \cap M_j = 0$ then we could replace $I'$ by $I' \cup \{j\}$, contradicting the maximality of $I'$. Hence $M_j \subseteq M'$ for all $M_j, j \in I$, and so $M \subseteq M'$. Since clearly $M' \subseteq M$ we have $M = M' = \sum_{i\in I'} M_i$, the sum being direct since $I' \in \mathcal{S}$. □

This proposition may be used to obtain information about the submodules and quotient modules of a semisimple module $M$.

**Corollary 1.5** *If $M$ is a semisimple module, then every submodule and every quotient module of $M$ is semisimple. Moreover, every submodule is a direct summand.*

**Proof:** Write $M$ as a direct sum of simple modules $M = \bigoplus_{i\in I} M_i$. If $M'$ is a submodule of $M$, then $M/M'$ is generated by the images $\overline{M}_i$ of the $M_i$ under the natural projection $M \longrightarrow M/M'$. Now if $\overline{M}_i \neq 0$, then $\overline{M}_i \approx M_i$ since $M_i$ is simple, so by the above proposition there exists $I'' \subseteq I$ such that $M/M' = \bigoplus_{i\in I''} M_i$; hence $M/M'$ is semisimple. It is now easy to check that

$$M = (\bigoplus_{i\in I''} M_i) \oplus M'$$

(see Exercise 15). Finally, $M'$ is semisimple because it is a quotient of the semisimple module $M$; morever, if $I' = I \backslash I''$, then

$$M' \approx M/\bigoplus_{i\in I''} M_i \approx \bigoplus_{i\in I'} M_i.$$

□

There is a partial converse to this corollary that provides a useful criterion for determining whether or not a module is semisimple :

**Proposition 1.6** *Let $M$ be a module such that every submodule of $M$ is a direct summand. Then $M$ is semisimple.*

**Proof:** The proof, with outline provided, is left as Exercise 17. □

# The Endomorphism Ring of a Semisimple Module

Any linear transformation of one finite-dimensional vector space into another can always be represented by a matrix, with composition of transformations corresponding to matrix multiplication. This way of describing linear transformations is extremely useful, and we wish to develop the idea more generally for semisimple modules.

The first result we prove will show how to represent $R$-linear maps between direct sums of $R$-modules (in particular free $R$-modules) by matrices with entries in $R$. The reader should keep in mind the special case when $R$ is a field. As we shall see in the discussion following the proposition, however, matrices which represent $R$-linear maps for noncommutative rings $R$ still have entries in $R$, but these entries must be multiplied in reverse order; that is, we should view the entries as elements of the opposite ring of $R$. Before discussing this more precisely, we prove the following

**Proposition 1.7** *Let $M$ be an $R$-module and let $S = End_R(M)$. For any positive integers $m, n$, there is a canonical isomorphism of abelian groups*

$$Hom_R(M^n, M^m) \approx S^{m\times n}$$

*such that the composition*

$$Hom_R(M^n, M^m) \times Hom_R(M^p, M^n) \longrightarrow Hom_R(M^p, M^m)$$

$$(f, g) \longmapsto f \circ g$$

*corresponds to matrix multiplication*

$$S^{m\times n} \times S^{n\times p} \longrightarrow S^{m\times p}$$

$$(A, B) \longmapsto AB$$

*In particular,* $End_R(M^n) \approx S^{n\times n} = \mathcal{M}_n(S)$ *is an isomorphism of rings.*

For a more general result, which shows how to represent homomorphisms of sums of different $R$-modules into other such sums, see Chapter 0, Exercise 10.

**Proof:** We'll give the setup and let the reader check the details. Given $f : M^n \longrightarrow M^m$, let $\alpha_{ij}$ be the composite

$$M \longrightarrow M^n \xrightarrow{f} M^m \longrightarrow M$$

where the first map is 'injection of the j-th summand' and the last map is 'projection onto the i-th factor'. This gives the correspondence $f \longmapsto [\alpha_{ij}]$, where $[\alpha_{ij}]$ is an $m \times n$ matrix with elements in $S$.

In the other direction, given $[\alpha_{ij}]$, we define

$$f(x_1, \ldots, x_n) = (y_1, \ldots, y_m) \qquad \text{where } y_i = \sum_{j=1}^{n} \alpha_{ij}\, x_j.$$

□

For an element $r$ of a ring $R$, let $T_r : R \longrightarrow R$ denote the $R$-linear map $T_r(x) = xr$ (note that the natural choice $T_r(x) = rx$ is not $R$-linear). This gives a function

$$\begin{aligned} R &\longrightarrow End_R(R) \\ r &\longmapsto T_r \end{aligned}$$

which fails to be a homomorphism of rings since multiplication is backwards, namely $T_r \circ T_s = T_{sr}$. If $R$ is commutative, then $T_{sr} = T_{rs}$, and

so this map does give a homomorphism. This homomorphism is one-to-one since $T_r = T_s$ implies in particular that $r = T_r(1) = T_s(1) = s$, and is onto since $f = T_{f(1)}$ for any $f \in End_R(R)$. Thus $End_R(R) \approx R$ if $R$ is commutative. In general, the problem of "backwards multiplication" is corrected by looking at the **opposite ring** $R^\circ$ of $R$, which has the same additive group as $R$, but has multiplication defined by $r \cdot s = sr$ (see Chapter 0, Exercise 25 for properties of the opposite ring). By the same argument, it is clear that $End_R(R) \approx R^\circ$ for any ring $R$. Note that this is consistent with the case when $R$ is commutative, for then $R \approx R^\circ$.

We now look at Proposition 1.7 in the special case of modules over a division ring. The theory of modules over a division ring $D$ is very much like the theory of vector spaces over a field. In particular, any $D$-module is a direct sum of copies of $D$ (by the usual proof for vector spaces over a field), and (by Proposition 1.7) we can represent any $D$-linear map $D^n \longrightarrow D^m$ as an $m \times n$ matrix with entries in $End_D(D) \approx D^\circ$; that is

$$End_D(D^n) \approx \mathcal{M}_n(End_D(D)) \approx \mathcal{M}_n(D^\circ).$$

Notice that if $D$ is a field then $D^\circ \approx D$, and we obtain the well-known result from linear algebra that linear transformations can be represented by matrices with entries in the base field, with composition of transformations corresponding to matrix multiplication.

We conclude this section with a theorem that gives us some idea of what the endomorphism ring of a semisimple $R$-module looks like for an arbitrary ring $R$. In order to do this we must make one additional (though not too restrictive) assumption. We will need

**Definition:** A semisimple module has **finite length** if it is a finite direct sum of simple modules.

This definition is a special case of the definition of finite length for arbitrary modules. For the more general definition of finite length, see the exercises in Chapter 0. The statements that follow also hold for the more general definition, although the proofs are a bit messier.

**Proposition 1.8** *If $M$ is a semisimple $R$-module of finite length, then $End_R(M)$ is isomorphic to a finite product of matrix rings over division rings.*

**Proof:** By grouping together isomorphic simple summands of $M$ we can write

$$M \approx \bigoplus_{i=1}^{k} M_i^{n_i}$$

with $M_i$ simple and $M_i \not\approx M_j$ if $i \neq j$ (the $M_i^{n_i}$ are called the **homogeneous** or **isotypic components** of $M$). Since $Hom(M_i, M_j) = 0$ for $i \neq j$, clearly any endomorphism of $M$ must take each isotypic constituent into itself. Thus we have

$$\begin{aligned} End_R(M) &\approx End_R(\textstyle\bigoplus_{i=1}^k M_i^{n_i}) \\ &\approx \textstyle\prod_{i=1}^k End_R(M_i^{n_i}) && \text{by Chapter 0, Exercises 8 and 9} \\ & && \text{and the above comment} \\ &\approx \textstyle\prod_{i=1}^k \mathcal{M}_{n_i}(End_R(M_i)) && \text{by Proposition 1.7.} \end{aligned}$$

and $End_R(M_i)$ is a division ring for each $i$ by Schur's Lemma. □

This proposition shows that for semisimple $R$-modules $M$, we can think of $End_R(M)$ as isomorphic to the ring of matrices of the form

$$\begin{pmatrix} A_1 & 0 & 0 & 0 \\ 0 & A_2 & 0 & 0 \\ & & \ddots & \\ 0 & 0 & 0 & A_n \end{pmatrix}$$

where $A_i$ is an $n_i \times n_i$ matrix with elements in the division ring $End_R(M_i)$. This is a particularly concrete way of describing semisimple $R$-modules.

## Semisimple Rings

This section introduces the concept of semisimple ring. Semisimple rings arise in diverse areas of mathematics such as number theory, representation theory, differential geometry and analysis. Understanding their structure will be one of our goals. Semisimple rings will also provide us with many examples of semisimple modules.

**Definition:** A ring $R$ is a **(left) semisimple ring** if $R$ is semisimple as a left $R$-module.

**Remark:** There is also an obvious notion of "right semisimple" . We shall soon see, however, that this notion coincides with that of "left semisimple", so we shall henceforth drop the qualifier "left".

We now give two other conditions which are equivalent to semisimplicity of a ring. This will be our first example of how the structure of a ring may be deduced from information about modules over that ring. For those not familiar with the definition of exact sequence or split exact sequence, see Chapter 0.

**Theorem 1.9** *Let $R$ be a ring. Then the following are equivalent :*
*(1) $R$ is a semisimple ring.*
*(2) Every $R$-module is semisimple.*
*(3) Every short exact sequence of $R$-modules splits.*

*Moreover, if these conditions hold then $R$ has finite length as an $R$-module and every simple $R$-module is isomorphic to a simple constituent of $R$. In particular there are only finitely many simple $R$-modules (up to isomorphism).*

**Proof:**

(1) implies (2): If $R$ is a semisimple $R$-module, then $\bigoplus_I R$ is semisimple for any such sum. Any $R$-module $M$ is the quotient of some free module $\bigoplus_I R$ (Chapter 0, Exercise 3), hence is semisimple since quotients of semisimple modules are semisimple (Corollary 1.5).

(2) implies (3): This follows immediately from the fact that every submodule of a semisimple module is a direct summand ( Corollary 1.5).

(3) implies (1): Given a submodule $I$ of $R$, looking at

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

shows that, by (3), $I$ is a direct summand of $R$. $R$ is thus semisimple by Proposition 1.6.

If the above three conditions hold, then $R \approx \bigoplus_{i \in I} M_i$ as modules for some simple $R$-modules $M_i$. But $R$ is finitely generated (by $1 \in R$) as an $R$-module, so $I$ is finite. Thus $R$ has finite length. If $M$ is a simple $R$-module, we have

$$\bigoplus_{i \in I} M_i \xrightarrow{\approx} R \longrightarrow M$$

with the second map onto (Proposition 1.1). Since $M$ is simple, only one of the maps $M_i \longrightarrow M$ is nonzero, and so must be an isomorphism. Thus the simple $R$- modules are precisely the $M_i$, and there are finitely many of them. □

It is worth re-emphasizing that the only simple $R$-modules are those occuring in the representation of $R$ as a direct sum of simple modules.

**Examples:**

1. Any division ring $D$ is semisimple because it has no proper (left) ideals; hence it is a simple $D$-module.

2. Theorem 1.9 says that semisimple rings are, as modules, finite direct sums of simple submodules. Since simple **Z**-module are just cyclic groups of prime order, and since $\mathbf{Z} \neq \sum_{finite} \mathbf{Z}/p\mathbf{Z}$ for any such finite sum, it follows that the ring **Z** is not semisimple. Indeed, the homogeneous (i.e., having just one homogeneous constituent) semisimple **Z**-modules are just the elementary $p$-groups, and the general semisimple **Z**-module is a direct sum of such.

3. If $F$ is a field, then $F[x]$ is not semisimple for reasons similar to the above.

4. One can check that $\mathbf{Z}/n\mathbf{Z}$ is semisimple if $n$ is square-free. Similarly, for a field $F$, $F[x]/(f)$ ($F$ a field) is semisimple if $f$ is square-free.

5. If $D$ is a division ring, $V$ a finite dimensional vector space over $D$, then the matrix ring $End_D(V)$ is semisimple. Further, all simple modules over $End_D(V)$ are isomorphic.

   **Proof:** Choose a basis $\{e_1, \ldots, e_n\}$ for $V$ and define

$$\begin{aligned} R = End_D(V) &\longrightarrow V \oplus \cdots \oplus V \\ f &\longmapsto (f(e_1), \ldots, f(e_n)) \end{aligned}$$

   We claim that the above map is an isomorphism of $R$-modules: It is a homomorphism since $\epsilon_v$, the evaluation map at $v$, is $R$-linear, as seen by

$$\begin{aligned} \epsilon_v(hf) &= (hf)(v) \\ &= h(f(v)) \\ &= h(\epsilon_v(f)). \end{aligned}$$

   The map is one-to-one since $f$ is determined by what it does to a basis, and is onto since, given any function on a basis, there exists an $f \in End_D(V)$ extending that function.

   Thus, since $V$ is a simple $End_D(V)$-module (see the example after Proposition 1.1), we see that $End_D(V)$ is a semisimple ring. By Theorem 1.9, every module over $End_D(V)$ is a direct sum of simple modules (namely copies of $V$). □

   Let us look at the above in terms of matrices, where we can give a convenient family of simple submodules of the semisimple module $\mathcal{M}_n(D^\circ) = End_D(V)$ which illustrates the decomposition concretely.

The spaces of column vectors

$$V_i = \begin{bmatrix} 0 & \cdots & a_{1i} & \cdots & 0 \\ \vdots & & a_{2i} & & \vdots \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & a_{ni} & \cdots & 0 \end{bmatrix}$$

are simple submodules of the semisimple module $\mathcal{M}_n(D^\circ) = End_D(V)$, and further $\mathcal{M}_n(D^\circ) = V_1 \oplus \cdots \oplus V_n$. Note again that the $V_i$ are mutually isomorphic, so there is a single simple module (up to isomorphism).

Note: This result is not true if $V$ is not finite-dimensional (see Exercise 28).

6. If $R$ and $S$ are semisimple rings, then $R \times S$ is semisimple. This can be seen from the fact that if $M$ is an $R \times S$-module, then $M = M_1 \oplus M_2$, where $M_1$ is an $R$-module and $M_2$ is an $S$-module (see Chapter 0, Exercise 6).

Examples 5 and 6 imply that, given division rings $D_i$ $(i = 1, \ldots, n)$ and finite dimensional vector spaces $V_i$ over $D_i$, $\prod_{i=1}^n End_{D_i}(V_i)$ is semisimple. For emphasis we state this as

**Proposition 1.10** *Any finite product of matrix rings over division rings is semisimple.*

## Wedderburn Structure Theorem

Theorem 1.9 says that a semisimple ring $R$ is isomorphic, as an $R$-module, to a finite sum of simple $R$-modules. We can also give such a decomposition of $R$ into rings instead of modules; in fact, an even more precise result can be given. Proposition 1.10 states that any finite product of matrix rings is semisimple. The fact that all semisimple rings are of this form is the content of the next theorem. This will be our second example of how the structure of a ring may be deduced from information about modules over that ring.

**Theorem 1.11 (Wedderburn Structure Theorem)** *Every semisimple ring $R$ is isomorphic to a finite direct product of matrix rings over division rings. If $R$ is commutative, then $R$ is isomorphic to a finite direct product of fields.*

**Proof:** Since $R$ is semisimple as a ring (and thus of finite length as an $R$-module, by Theorem 1.9) we have, by Proposition 1.8, that $End_R(R)$ is isomorphic to a finite product $\prod \mathcal{M}_{n_i}(D_i)$ of matrix rings over division rings $D_i$. But $End_R(R) \approx R^\circ$. Thus

$$R \approx (R^\circ)^\circ \approx \prod [\mathcal{M}_{n_i}(D_i)]^\circ$$
$$\approx \prod \mathcal{M}_{n_i}(D_i^\circ).$$

The last isomorphism comes from the fact that $\mathcal{M}_n(D)^\circ \approx \mathcal{M}_n(D^\circ)$, as can be seen by using the transpose. The second statement of the theorem is clear. □

Before elaborating on the Wedderburn Structure Theorem, we give one immediate consequence which makes life a bit less complicated.

**Corollary 1.12** *A ring is left semisimple if and only if it is right semisimple.*

Thus we refer only to semisimple rings without mention of left or right.

**Definition:** A ring is called **simple** if it has no non-trivial two-sided ideals. This is, in general, weaker than saying that the ring is simple as a module over itself; any ring which is simple as a module over itself is a simple ring, but not conversely. Exercise 5 of this chapter shows that a ring of $n \times n$ matrices over a division ring is simple, although it may contain many nontrivial left ideals. It should be noted that some authors (e.g., Lang and Bourbaki) define "simple" for rings so that "simple" implies semisimple. As we shall see, one more condition needs to be met for our simple rings to be semisimple.

Combining the fact that matrix rings are simple with the Wedderburn Structure Theorem, we see that

*Every semisimple ring $R$ is isomorphic to a finite product of simple rings $R_1, \ldots, R_n$.*

We can think of each $R_i$ as $0 \times \ldots \times R_i \times \ldots \times 0$ sitting inside of $R = R_1 \times \ldots \times R_n$, so that each $R_i$ is a two-sided ideal in $R$ (but not a subring!) and thus an $R$-submodule of $R$. It is easy to check that if $i \neq j$ then $R_i \not\approx R_j$ as $R$-modules, even if $R_i \approx R_j$ as rings (Chapter 0, Exercise 7).

We also know what all of the simple $R$-modules are: each $R_i$ is isomorphic to a matrix ring $\mathcal{M}_{n_i}(D_i)$, and, being simple, has a unique isomorphism class of simple modules (by the Structure Theorem for Simple Artinian Rings to follow). The unique isomorphism class of simple left (right) $R_i$-modules is the space generated by any column (row) vector (check this). Thus $R$ has exactly $n$ isomorphism classes of simple modules. This follows

from the fact that if $M$ is an $R \times S$-module, then $M = M_1 \oplus M_2$, where $M_1$ is an $R$-module and $M_2$ is an $S$-module (Chapter 0, Exercise 6).

The Wedderburn Structure Theorem is a special case of a more general theory of rings of projective dimension zero. For more information about this topic, see Chapter 7.

We have shown that every semisimple ring can be written as a direct product of simple rings. The following theorem tells us that we can do this uniquely.

**Theorem 1.13 (Uniqueness Theorem for Semisimple Rings)** *If*

$$R = \prod_{i=1}^{n} R_i \qquad \text{and} \qquad R = \prod_{j=1}^{m} R'_j$$

*are two product decompositions of a ring $R$, where each $R_i$ and $R'_j$ is a simple ring, then $n = m$ and each $R_i$ is some $R'_j$.*

**Remark:** The following proof will show that these simple factors are unique in the sense that each $R_i$ really is equal to, not just is isomorphic to, some $R'_j$.

**Proof:** First note that for each $i$, $R_iR = R_i$, since we may think of each $R_i$ (and $R'_j$) as a two-sided ideal in $R$. Applying this to the equation $R = \prod_{j=1}^{m} R'_j$ gives $R_i = \prod_{j=1}^{m} R_iR'_j$. Now each $R_iR'_j$ is a two-sided ideal of $R_i$ and is thus either zero or $R_i$. Since every $R_iR'_j$ isn't zero, there is an $R'_j$ with $R_i = R_iR'_j$. Now $R_i = R_iR'_j$ is also a two-sided ideal of $R'_j$, and so must equal $R'_j$. Thus we see that $R_i = R'_j$. □

There is an analogous, but weaker, uniqueness theorem for semisimple modules, the proof of which we leave as an exercise (see Exercise 25).

## Simple Rings and Further Applications

It follows from the definitions that any simple module is semisimple. Looking at the way we defined these concepts for rings, however, the analogous fact is not clear. In fact it is not true that every simple ring is semisimple! (See Exercise 28 for an example.) The problem is that it is possible for a ring (even a simple one) to contain an infinite descending sequence of distinct left ideals $I_1 \supset I_2 \supset I_3 \supset \cdots$, but Theorem 1.9 shows that any semisimple ring has finite length, and so no such descending chain of ideals exists in a semisimple ring. If we assume that this does not happen in the simple ring $R$, however, then it will be true that $R$ is semisimple. A ring satisfying such a descending chain condition is called **left artinian**. For

those not familiar with artinian (and noetherian) rings and modules, see the section on chain conditions in the exercises of Chapter 0 for additional information.

Before proving that any simple artinian ring is semisimple, we shall introduce two useful concepts that will aid in our understanding of the structure of rings.

For a vector space $V$ over a field $F$, $V$ can be written as a direct sum of one-dimensional subspaces, each of which is isomorphic (as an $F$-module) to the simple module $F$. Thus $V$ can be broken up into simple pieces each of which looks the same. The next definition generalizes this concept.

**Definition:** A semisimple module is called **homogeneous** if it is a direct sum of a collection of simple modules all of which are isomorphic to a fixed simple module $S$. We also say that the module is homogeneous or **isotypic of type S**.

To prove the Structure Theorem for Simple Artinian Rings, we need a lemma concerning endomorphisms of homogeneous semisimple modules. Recall that a submodule $M' \subseteq M$ is said to be **stable** under the endomorphism $\phi : M \longrightarrow M$ if $\phi(M') \subseteq M'$. For homogeneous semisimple modules, we can say exactly which submodules are stable under all endomorphisms; namely, we have :

**Lemma 1.14** *Let $M$ be a homogeneous semisimple module. Then the only submodules of $M$ that are stable under all endomorphisms are $0$ and $M$.*

**Proof:** Suppose $M'$ is a proper non-zero submodule. Since $M$ is semisimple, $M'$ is a direct summand, say $M = M' \oplus M''$. Note that both $M'$ and $M''$ are semisimple and in fact are homogeneous of the same type as $M$ (see the proof that submodules and quotients of semisimple modules are semisimple in Corollary 1.5). Hence $Hom(M', M'') \neq 0$. But then it is easy to find endomorphisms of $M$ which don't stabilize $M'$, for example the composition

$$M \xrightarrow{proj.} M' \xrightarrow{\neq 0} M'' \hookrightarrow M.$$

□

The converse to this lemma is also true, as is shown in Exercise 11. That is, if $0$ and $M$ are the only submodules of $M$ which are stable under all endomorphisms of $M$, then $M$ is semisimple and homogeneous.

For a vector space $V$ over a field $F$, no non-zero scalar annihilates a non-zero vector; that is, any (non-zero) one-vector set is linearly independent. The more general notion for modules is the following :

**Definition:** An $R$-module $M$ is said to be **faithful** if, for every $r \in R$, $rM = 0$ implies that $r = 0$.

The following theorem ties together a few ways we have been looking at the structure of rings, and in particular proves our claim that any simple artinian ring is semisimple. This theorem provides another nice example of the interplay between the structure of a ring and the structure of modules over that ring.

**Theorem 1.15 (Structure Theorem for Simple Artinian Rings)** *Let $R$ be a ring. Then the following are equivalent :*
*(1) $R$ is a simple artinian ring.*
*(2) $R$ is isomorphic to a matrix ring over a division ring.*
*(3) $R$ is semisimple and all simple modules over $R$ are isomorphic.*
*(4) $R$ is homogeneous and semisimple as an $R$-module.*
*(5) $R$ is artinian and has a faithful simple module.*

This theorem is sometimes called the Wedderburn-Artin Theorem .

**Proof:** (5) implies (4): Let $M$ be a faithful simple module. We'll show that $R$ is isomorphic to a submodule of $M^n$ for some $n$. Consider all $R$-homomorphisms $f : R \longrightarrow M^n$ for various $n$, and choose one with minimal kernel (we can do this since $R$ is artinian). We claim that $f$ is one-to-one, for if $f(r) = 0$ and $r \neq 0$, then since $M$ is faithful there is an $m \in M$ with $rm \neq 0$. Define

$$R \longrightarrow M^n \oplus M$$

by

$$x \longmapsto (f(x), xm)$$

This map has smaller kernel than $f$, giving a contradiction. Thus $f$ is one-to-one and so $R$ is a submodule of the homogeneous semisimple module $M^n$. Hence $R$ is homogeneous and semisimple.

(4) implies (3): This follows immediately from the definitions and Theorem 1.9.

(3) implies (2): This follows immediately from the Wedderburn Structure Theorem and the comments following it.

(2) implies (1): This is simply the fact that every matrix ring over a division ring is both simple (Exercise 5) and artinian (Chapter 0,Exercise 48).

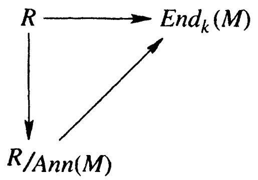
(1) implies (5): Note that for any module $M$, $Ann(M) = \{r \in R | rM = 0\}$ is a two-sided ideal of the simple ring $R$ and $1 \notin Ann(M)$, so $Ann(M) = 0$. Thus any $R$-module is faithful. Since $R$ is artinian, $R$ has some simple module; in fact, any module has a simple submodule, for any descending chain of ideals must eventually stabilize, and the module to which the sequence stabilizes must clearly be simple. Thus $R$ has a faithful simple module. This completes the proof of the Theorem. □

**Remark:** It is easily shown (see Exercise 18) that if $R$ satisfies the hypotheses of Theorem 1.15 and $M$ is a simple $R$-module with endomorphism ring $D$ (remember $D$ will be a division ring), then the structure map $R \longrightarrow End_D(M)$ is an isomorphism. This gives an explicit realization of (2).

We apply the ideas of this chapter to prove a classical result due to Burnside.

**Corollary 1.16 (Burnside)** *Let $R$ be an algebra over a field $k$ and let $M$ be a simple $R$-module such that $dim_k(M) < \infty$. Also suppose that $End_R(M) = k$ (e.g., if $k$ is algebraically closed, cf. Corollary 1.3). Then the structure map $R \longrightarrow End_k(M)$ is onto.*

**Proof:** The diagram




commutes, where the homomorphism from $R$ to $End_k(M)$ is the structure map of $M$ as an $R$-module. Now

(1) $M$ is a faithful $R/Ann(M)$-module (always), and hence
(2) $R/Ann(M) \hookrightarrow End_k(M)$ and the latter is finite dimensional over $k$ since $M$ is finite dimensional over $k$. Thus $R/Ann(M)$ is artinian since it has finite dimension.

Now (1) and (2) are just condition (5) of Theorem 1.15 for the ring $R/Ann(M)$, hence $R/Ann(M) \approx End_k(M)$ via Remark (2) above, and we are done. □

We now give a corollary which will be useful later on in our study of the Brauer group. We give this corollary, which shows that every element in the Brauer group (defined in Chapter 4) has an inverse, in order to demonstrate some of the techniques used in this chapter.

**Corollary 1.17** *Let $k$ be a field. Let $R$ be a simple $k$-algebra of finite dimension $n$ whose center is $k$. Then $R \otimes_k R^\circ \approx \mathcal{M}_n(k)$.*

**Proof:** $R$ is an $R$-$R$ bimodule relative to $k$, hence an $R \otimes_k R^\circ$-module (Chapter 0, Exercise 28). It is a simple $R \otimes_k R^\circ$-module since it has no

non-zero two-sided ideals (two-sided ideal = $R \otimes_k R^\circ$-submodule of $R$). Consideration of the map

$$End_{R\otimes_k R^\circ}(R) \longrightarrow Z(R)$$

$$f \longmapsto f(1)$$

shows that

$$End_{R\otimes_k R^\circ}(R) \approx Z(R) = k.$$

So by Corollary 1.16

$$R \otimes_k R^\circ \longrightarrow End_k(R) \approx \mathcal{M}_n(k)$$

is onto. But both the domain and the range have $k$-dimension $n^2$, and so the map is an isomorphism. □

## Summary

Throughout this chapter we have seen several characterizations of semisimple rings. In the exercises, we will introduce other properties of a ring which are equivalent to semisimplicity. Since it is useful to keep all of these properties in mind when looking at such rings, we give a summary of several properties which characterize semisimple rings :

**Theorem 1.18** *For a ring R the following are equivalent:*
*(1) R is a semisimple ring; i.e., R is semisimple as a left R-module.*
*(2) Every left R-module is semisimple.*
*(3) Every short exact sequence of left R-modules splits.*
*(4) Every left R-module is projective.*
*(5) Every left R-module is injective.*
*(6) R is ring isomorphic to a finite product of matrix rings over division rings.*
*(7) R is the direct sum of a finite number of simple left ideals*

$$R = \bigoplus_{i=1}^{n} L_i$$

*where each $L_i$ is a simple (as a submodule) left ideal and $L_i = Re_i$, where $\{e_i\}_{i=1}^n$ is a set of orthogonal idempotents such that $e_1 + e_2 + \cdots + e_n = 1$.*
*(8) R is artinian and has vanishing Jacobson radical.*

*Moreover, (1)-(5) hold with "left" replaced by "right".*

An explanation of (4) and (5) will be given in the exercises, and an explanation of (8) will be given in Chapter 2. These conditions are included here for completeness. The proof of this theorem (except for (8)) is contained in this chapter partly in the exposition and partly in the exercises.

# Exercises

## A Lonely, Ungroupable Exercise

1. Let $D$ be a division algebra which has finite dimension over the field $k$. For each $a \in D$ show there is a monic polynomial in $k[x]$ which has $a$ as a root. Conclude that if $k$ is algebraically closed, then $k = D$. Note that this proves Corollary 1.3.

### Simplicity

2. Let $R$ be a ring (with 1) such that the only left ideals of $R$ are 0 and $R$. Show that $R$ must be a division ring; that is, if $R$ is simple as a left $R$-module, then $R$ is a division ring. If the hypothesis that $R$ has an identity is dropped, the result no longer holds. Give an example to show this. In fact, the type of example you give is unique.

3. Show that the assumption "every non-zero element is a generator" in Proposition 1.1 is necessary.

4. Determine all simple $R$-modules, where
   (a) $R = \mathbf{Z}$.
   (b) $R = \mathbf{C}[x]$.
   (c) $\mathbf{Q}/(x^3 - 5)$
   (c) $R$ is a principal ideal domain.
   (d) $R = \mathbf{C}[x, y]$.
   (e) $R$ is the set of continuous, real-valued functions with domain $[0, 1]$.

5. Show that the only two-sided ideals of $\mathcal{M}_n(R)$ are of the form $\mathcal{M}_n(I)$ for some two-sided ideal $I$ of $R$. Conclude that $\mathcal{M}_n(R)$ is a simple ring if and only if $R$ is a simple ring. [Hint: The following may be useful: Let $e_{ij}$ denote the $n \times n$ matrix with 1 in the $i, j$ position and zeros elsewhere. These matrices are called the **elementary matrices** of $\mathcal{M}_n(R)$. Clearly $\{e_{ij} : 1 \le i, j \le n\}$ is a basis for $\mathcal{M}_n(R)$ considered as an $R$-module. So every element of $\mathcal{M}_n(R)$ can be written uniquely as $\sum a_{ij}e_{ij}$, and the $e_{ij}$ can be multiplied via the formula

$$e_{ij}e_{kl} = \begin{cases} 0 & \text{if } j \neq k \\ e_{il} & \text{if } j = k. \end{cases}$$

Note also that elementary row operations correspond to left multiplication by elements of the form

$$E_{ij}(r) = I + re_{ij} \quad r \in R, i \neq j$$

where $I$ denotes the $n \times n$ identity matrix. Similarly, column operations correspond to right multiplication by such elements.]

**Remark:** The above exercise can be viewed as a very special case in Morita theory. Morita theory provides a set of data (called a **Morita context**) which gives a categorical equivalence between the category of $R$-modules and the category of $S$-modules, where $R$ and $S$ are rings forming part of a Morita context. In particular, $R$ and $\mathcal{M}_n(R)$ are related by a Morita context. For more on Morita theory, see Jacobson's *Basic Algebra II.*

### Semisimplicity

6. Show that the $\mathbf{Z}$-module $\mathbf{Q}$ is neither semisimple nor has a simple quotient. In fact, show that $\mathbf{Q}$ is **indecomposable** : it is not the direct sum of two proper $\mathbf{Z}$-submodules.

7. Show that the following conditions are equivalent for a semisimple module $M$ :
(i) $M$ is finitely generated.
(ii) $M$ is a direct sum of a finite number of simple submodules.
(iii) $M$ has finite length.
(iv) $M$ satisfies both the ACC and DCC.

   In particular note that, for a vector space, length equals dimension. Note that the equivalence of (iii) and (iv) is Exercise 46 of Chapter 0.

8. Prove that the homomorphic image of a semisimple ring is semisimple.

9. Let $R$ be a ring and $M$ a semisimple $R$-module. Let $S$ and $S'$ be isomorphic simple submodules of $M$ via the isomorphism $g : S \longrightarrow S'$.

   (a) Show that there is an $R$-isomorphism $f : M \xrightarrow{\approx} M$ such that the restriction of $f$ to $S$ is the given isomorphism $g$; in particular, $f(S) = S'$.

   (b) Show that this isn't true if $S$ and $S'$ are isomorphic but otherwise arbitrary. [Hint : look at an infinite-dimensional vector space and an infinite-dimensional proper subspace.]

10. Let $N$ be a submodule of the $R$-module $M$. If $N$ and $M/N$ are semisimple, does it follow that $M$ is semisimple?

11. Let $M$ be a module. Show that 0 and $M$ are the only submodules of $M$ stabilized by every endomorphism of $M$ if and only if $M$ is semisimple and homogeneous(cf. Lemma 1.14).

12. Prove that a module $M$ is semisimple if and only if every cyclic submodule of $M$ is semisimple.

**Some Centers**

13. Let $R$ be a ring. The **center** of $R$, denoted $Z(R)$, is $\{z \in R | zr = rz$ for all $r \in R\}$. $Z(R)$ is a commutative subring of $R$.

(a) Show that $Z(R \times S) \approx Z(R) \times Z(S)$.

(b) Show that $Z(\mathcal{M}_n(R)) \approx Z(R)$.

(c) Show that $Z(D)$ is a field if $D$ is a division ring.

(d) Compute $Z(\mathcal{T}_n(R))$ for $\mathcal{T}_n(R)$ the ring of $n \times n$ upper triangular matrices over $R$.

(e) Show that the center of a semisimple ring is a product of fields, hence is semisimple.

(f) Let $D$ be a division ring and $V$ a non-zero vector space over $D$. Let $k = Z(D)$ and $R = End_D(V)$. There is a homomorphism $k \rightarrow R$ given by the action of $k$ on $V$ by scalar multiplication. Show that this induces an isomorphism $k \approx Z(R)$.

(g) Let $k$ be a field and let $G$ be a group. Describe $Z(k[G])$. [Hint: If $g \in G$ has only finitely many conjugates, consider the element $C_g$ in $k[G]$ which is the sum of the conjugates of $g$.]

14. Let $R$ be a semisimple artinian ring.

(a) Prove that, if $I$ is a two-sided ideal of $R$, then the canonical homomorphism $Z(R) \longrightarrow Z(R/I)$ is surjective.

(b) Let $M$ be a left $R$-module and let $S = End_R(M)$. Prove that the homomorphism

$$T : Z(R) \longrightarrow Z(S)$$

defined by

$$mT(r) = rm \quad \text{for } r \in R, m \in M$$

is surjective. Note that we view $M$ as an $R-S$-bimodule.

(c) Assume now that $R$ is simple artinian, and let $D$ be the division ring such that $R \approx \mathcal{M}_n(D)$. Prove that $Z(R) \approx Z(D)$ as fields. [Note that this can be deduced from part (b) or shown directly.]

## Direct Summands

15. Let $M$ be an $R$-module and $M'$ a submodule. Prove that $M'$ is a direct summand of $M$ if and only if $M$ has a submodule $M''$ which maps isomorphically onto $M/M'$ under the canonical projection $M \to M/M'$.

16. If $M'$ is a direct summand of $M$, prove that any two complements for $M'$ are isomorphic (recall that a **complement** of $M'$ in $M$ is a submodule $N$ with $M = M' \oplus N$). Give an example to show that two complements are not necessarily equal.

17. Let $M$ be a module such that every submodule is a direct summand. Show that $M$ is semisimple as follows:

    (a) Show that every submodule of $M$ inherits the property that each of its submodules is a direct summand.

    (b) Show that $M$ contains a simple submodule : Choose any finitely generated non-zero submodule $M' \subseteq M$ (e.g., $M'$ could be cyclic). Let $M'' \subset M'$ be a maximal submodule not equal to $M'$ (why do such submodules exist?). Hence $M'/M''$ is simple and by (a) there is an $X \subset M'$ with $M' = M'' \oplus X$ and with $X \approx M'/M''$ simple.

    (c) Let $M_1$ be the submodule of $M$ generated by all simple submodules, which is thus a direct sum of simple modules. Then $M = M_1 \oplus M_2$ for some submodule $M_2$. Applying (a) and (b) we see that if $M_2 \neq 0$, then it contains a simple submodule and we get a contradiction.

## More Information from the Wedderburn Structure Theorem

18. Let $R$ be a semisimple ring, let $\{M_1, \ldots, M_n\}$ be a set of representatives for the isomorphism classes of simple $R$-modules, and let $D_i = End_R(M_i)$. The action of $R$ on $M_i$ defines a homomorphism $\phi_i : R \to End_{D_i}(M_i)$. Combining these gives a homomorphism $\Phi : R \to \prod_{i=1}^{n} End_{D_i}(M_i)$. Prove that $M_i$ is finite dimensional over $D_i$ and that $\Phi$ is an isomorphism.

19. Prove that if $R$ is a commutative semisimple ring, then the canonical map $R \to \prod_I R/I$ is an isomorphism, where $I$ ranges over the maximal ideals of $R$.

20. With the notation of Exercise 18, let $n_i = dim_{D_i} M_i$. Prove that $n_i$ is the multiplicity with which $M_i$ occurs in $R$, regarded as a left $R$-module.

21. Prove that if $R$ is a semisimple ring then the isotypic components of $R$ are the minimal two-sided ideals of $R$. Prove that every two-sided

ideal of $R$ is a product of these and conversely. Note that the isotypic components are not subrings.

22. (a) Prove that $R$ is a semisimple ring if and only if $R$ is the direct sum of a finite number of simple left ideals

$$R = \bigoplus_{i=1}^{n} L_i$$

where each $L_i$ is a simple (as a submodule) left ideal and $L_i = Re_i$, where $\{e_i\}_{i=1}^{n}$ is a set of orthogonal idempotents such that $e_1 + e_2 + \ldots + e_n = 1$.

(b) Prove that if $\{e_1, \ldots, e_m\}$ is a set of orthogonal idempotents in $\mathcal{M}_n(D)$, $D$ a division ring, then $m \leq n$.

23. This exercise provides a sketch of a clever proof, due to M. Rieffel, of part of the Structure Theorem for Simple Artinian Rings. Let $M \neq 0$ be a left ideal of a simple ring $R$. Viewing $M$ as a left $R$-module, let $S = End_R(M), T = End_S(M)$, and $\psi : R \longrightarrow T$ be the natural homomorphism. Assume that $R$ possesses no nonzero proper two-sided ideals, so that $\psi$ is injective.

(a) Show that $\psi(M)$ is a left ideal of $T$. [Hint: Show that the mapping

$$\begin{aligned} M &\longrightarrow T \\ x &\longmapsto \psi(x) \end{aligned}$$

is a homomorphism of $T$-modules by using the fact that right multiplication by elements of $M$ yields elements of $S$.]

(b) Show that $\psi(R)$ is a left ideal of $T$. [Hint: Observe that $MR = R$ and apply $\psi$ and part (a).]

(c) Show that $\psi$ is an isomorphism.

24. Let $A$ be a simple $k$-algebra with center $k$ such that $[A : k] = p^2$ with $p$ a prime. Prove that either $A$ is a division algebra or $A \approx \mathcal{M}_p(k)$.

### Uniqueness Theorem for Semisimple Modules

25. Prove the Uniqueness Theorem for Semisimple Modules: If $M$ is an $R$-module and if

$$M = \bigoplus_{i=1}^{n} M_i \quad \text{and} \quad M = \bigoplus_{j=1}^{m} M'_j$$

are two direct sum decompositions of $M$ with simple summands $M_i$ and $M'_j$, then $n = m$ and there is a permutation $\pi$ of $\{1, \ldots, n\}$ with

$M_i \approx M'_{\pi(i)}$ for each $i = 1, \ldots, n$. [Hint : induct on the smaller of $m$ and $n$.]

26. (a) Show that the Uniqueness Theorem for Semisimple Modules is not true if we replace "is isomorphic to" by "is equal to", in contrast with the Uniqueness Theorem for Semisimple Rings. [Hint : Show that if $M = \mathbf{R}^2$ is viewed as an $\mathbf{R}$-module, then there are infinitely many ways to decompose $M$ as the direct sum of two simple submodules.]

    (b) Show that the ring $R$ of $2 \times 2$ matrices over the real numbers has an infinite number of distinct proper left ideals, any two of which are isomorphic as left $R$-modules. Then show that there are infinitely many distinct pairs $(I, I')$ of minimal left ideals of $R$ with $R = I \oplus I'$ as modules (remember that minimal left ideals correspond to simple left $R$-modules).

### Maschke's Theorem

27. Let $k$ be a field and $G$ be a finite group.

    (a) Let $M$ be a $k[G]$-module with submodule $N$. Since $k$ is a field, we know by Theorem 1.9 that the short exact sequence

$$0 \longrightarrow N \longrightarrow M \xrightarrow{p} M/N \longrightarrow 0$$

    splits as a sequence of $k$-modules (here $p$ is the canonical projection). Denote the splitting by $s : M/N \longrightarrow M$. Clearly there is no reason to believe that $s$ is a homomorphism of $k[G]$-modules.

    Define $S : M/N \longrightarrow M$ by the formula $S(x) = \sum_{g \in G} gs(g^{-1}x)$. Compute $p \circ S$.

    (b) Show that if $|G|$ is invertible in $k$, then there is a $k[G]$-splitting of the above sequence. Conclude that $k[G]$ is a semisimple ring.

    **Remarks :** This result, known as "Maschke's Theorem", is of fundamental importance for representation theory. Given a group $G$, we study $\mathbf{C}[G]$, which is just (by Maschke's Theorem and Wedderburn's Theorem) a product of algebras of the form $\mathcal{M}_n(\mathbf{C})$. Since we understand completely the structure of semisimple $\mathbf{C}$-algebras, the stratagem of embedding a mysterious object under study (the group $G$) into an object with a richer and therefore better-understood structure (the algebra $\mathbf{C}[G]$) can be expected to yield great dividends. In fact, many important theorems in the modern structure theory of finite groups are proved by representation-theoretic methods. See Chapter 6 for more on this, in particular for an application of Maschke's Theorem in proving Burnside's $p^a q^b$ theorem, a much celebrated result in group theory.

For those who know some analysis, think of $G$ as a discrete topological group with the counting measure $\mu$ normalized to be a probability measure; i.e., for $X \subseteq G$, $\mu(X) = \frac{\text{card}(X)}{|G|}$, so $\mu(G) = 1$. Then sums can be written as integrals; e.g., $\frac{1}{|G|}\sum_g a_g$ becomes $\int_G a(g)d\mu(g)$. Then the formula for the above splitting assumes the form :

$$\frac{1}{|G|}S(x) = \frac{1}{|G|}\sum_{g\in G} gs(g^{-1}x) = \int_G gs(g^{-1}x)d\mu(g).$$

This should look familiar - it's just the convolution of the identity with the map $s$. In fact, if $G$ is any compact topological group, there exists a unique left-invariant measure (i.e., $\mu(X) = \mu(gX)$ for all measurable $X \subseteq G$) with $\mu(G) = 1$, called the **Haar measure** on $G$. For example, the Haar measure on Euclidean space $\mathbf{R}^n$ is Lebesgue measure, and the Haar measure on the circle $S^1$ is the usual "$\frac{1}{2\pi}\cdot$ arclength" measure. The fundamental facts about group representations work just as well in this setting. Indeed, various formulae arising in the representation theory of finite groups are called "Fourier inversion" formulae, because that's exactly what's happening.

(c) Prove the converse of part (b). [Hint : Look at the exact sequence

$$0 \longrightarrow A \longrightarrow k[G] \xrightarrow{\epsilon} k \longrightarrow 0$$

where $\epsilon$ is the 'augmentation map' $\epsilon(\sum r_g g) = \sum r_g$ and $A$ is the kernel of $\epsilon$ ($A$ is often called the **augmentation ideal** of $k[G]$). Here $k$ is viewed as a $k[G]$ – *module* via $\epsilon$. Show that this exact sequence doesn't split when the characteristic of $k$ divides $|G|$.]

### Some Counterexamples

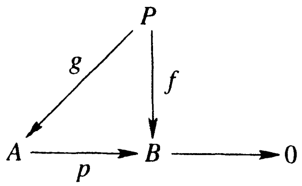
28. (a) If $V$ is a vector space of countably infinite dimension over a field $k$, show that the set of finite rank operators (i.e., those elements of $End_k(V)$ whose image is finite dimensional) forms a two-sided ideal in $End_k(V)$; hence $End_k(V)$ is not simple, in contrast to the fact that finite endomorphism rings of finite dimensional vector spaces are simple.

(b) Use part (a) to construct a simple ring which is not semisimple.

### Projective and Injective Modules

29. A module $P$ is called **projective** if any of the following three equivalent conditions holds :

(i) Given a homomorphism $f : P \longrightarrow B$ and a surjective homomorphism $p : A \longrightarrow B$, there exists a homomorphism $g : P \longrightarrow A$ making the following diagram commutative :




(ii) Every surjection $p : M \longrightarrow P$ splits, i.e., there is a homomorphism $s : P \longrightarrow M$ such that $ps = 1_P$.

(iii) $P$ is a direct summand of some free module $F$.

(a) Show that these three conditions are equivalent.

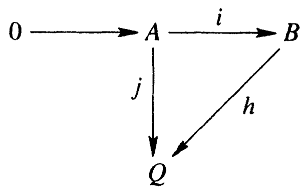
(b) Show that an arbitrary sum of modules is projective if and only if each of the summands is projective.

30. (a) Show that the projective **Z**-modules are precisely the free abelian groups; i.e., every projective **Z**-module is free. Generalize this to principal ideal domains.

(b) Let $R$ be the ring of two-by-two matrices over a field $k$, and let $I$ be the left ideal of $R$ consisting of matrices whose second column is zero. Show that the left $R$-module $I$ is projective but not free.

31. A module $Q$ is called **injective** if either of the following equivalent conditions holds :

(i) Given a homomorphism $j : A \longrightarrow Q$ and an injective homomorphism $i : A \longrightarrow B$, there exists a homomorphism $h : B \longrightarrow Q$ making the following diagram commutative :




(ii) Every injection $i : Q \longrightarrow M$ splits.

(a) Show that these two conditions are equivalent.

(b) Show that an arbitrary product of modules is injective if and only if each factor is.

**Remark :** Injectivity is a concept "dual" to projectivity; that is, the respective parts (i) and (ii) of the equivalent definitions are obtained from each other by reversing the direction of the arrows. Is there an analogue (or rather dual) to definition (iii) of Exercise 29 for injective modules?

32. Prove that every vector space over a division ring is both projective and injective.

33. Let $R$ be a ring. Show that the following statements are equivalent :

    (i) Every $R$-module is projective.

    (ii) Every short exact sequence of $R$-modules splits.

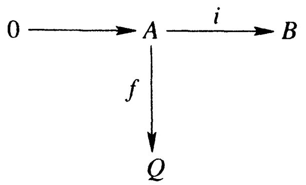
    (iii) Every $R$-module is injective.

    In view of Theorem 1.9, this gives us two more equivalent definitions of a semisimple ring.

34. Prove that $\mathbf{Q}$ is not a projective $\mathbf{Z}$-module, thus providing another proof that $\mathbf{Z}$ is not a semisimple ring.

35. Projective modules are quite common, whereas injective modules, though still extremely useful in many contexts, are harder to come by. This exercise gives a way of recognizing injective modules. Prove the following : The $R$-module $Q$ is injective if and only if for each left ideal $L$ of $R$, every homomorphism of $L$ to $Q$ can be extended to a homomorphism of $R$ to $Q$. [Hint : One direction is trivial. For the other direction proceed as follows :

    (i) Given a diagram




consider the collection $\mathcal{S}$ of all pairs $(B_j, f_j)$ where $image(i) \subset B_j \subset B$ and $f_j : B_j \longrightarrow Q$ satisfies $f_j i = f$. Partially order $\mathcal{S}$ by saying that $(B_j, f_j) \geq (B_k, f_k)$ if both $B_j \supset B_k$ and the restriction of $f_j$ to

$B_k$ is $f_k$. Apply Zorn's Lemma to get a maximal element of $\mathcal{S}$; call it $(B_0, f_0)$.

(ii) Now show that $B_0 = B$ : if $B_0 \neq B$, choose $c \in B$ with $c \notin B_0$ and let $L = \{r \in R | rc \in B_0\}$, a left ideal of $R$. Show that the formula $g(b) = f_0(bc)$ defines a homomorphism from $L$ to $Q$. Apply the hypothesis to get a homomorphism $g' : R \longrightarrow Q$. If $rc \in B_0$, show that $f(rc) = rg'(1)$. Let $B' = B_0 + Rc$, which contains but is not equal to $B_0$. Show that $f' : B' \longrightarrow Q$ given by the formula $f'(b_0 + rc) = f_0(b_0) + rg'(1)$ is a well-defined homomorphism which restricts to $f_0$ on $B_0$. This should yield a contradiction and conclude the proof.]

36. An abelian group $A$ is **divisible** if for all $a \in A$ and $n \in \mathbf{Z}, n \neq 0$, there exists $b \in A$ such that $a = nb$.

(a) Show that direct sums, homomorphic images, and direct summands of divisible groups are divisible.

(b) Show that an abelian group is divisible if and only if it is injective as a $\mathbf{Z}$-module.

37. (a) Show that the additive groups $\mathbf{Q}, \mathbf{R}$, and $\mathbf{C}$ are divisible.

(b) Show that $\mathbf{Q}/\mathbf{Z}$ and direct factors of $\mathbf{Q}/\mathbf{Z}$, for example the $p$-torsion subgroups $\mathbf{Z}_{p^\infty} = \{r \in \mathbf{Q} : p^n r \in \mathbf{Z} \text{ for some } n\}$ , are divisible.

(c) Show that no finite group is divisible. Show that no free abelian group is divisible.

# 2

# The Jacobson Radical

In Chapter One we developed a structure theory for semisimple rings, as summarized in Theorem 1.18. This theory used, for the most part, properties of modules over a semisimple ring in order to characterize such a ring. In this chapter, we give a more intrinsic characterization of semisimple rings.

What follows is part of a general theme in any structure theory. The idea is to single out some "undesirable" property of the object one wishes to study; in our case the information is captured by the Jacobson radical of a given ring. One then studies only those objects which don't have this property; for example, those rings whose radical is zero. This can be a tricky business, for one must strike a balance between studying a class of objects large enough to be interesting and useful, yet small enough to be tractable. A good example of such objects, as we have seen, are semisimple rings, and it is this class of objects we are most interested in. Our explorations using this philosophy will also provide us with valuable information about rings which are not semisimple.

## Another Characterization of Semisimple Rings

We understand vector spaces over fields quite well. One nice property of such modules is that no non-zero scalar annihilates a non-zero vector, and in particular does not annihilate the entire module; that is, a field acts faithfully on any vector space over that field (recall that an $R$-module $M$ is **faithful** if $ann(M) = 0$). Moving from the situation of a field to an arbitrary ring $R$, we want to come up with an algebraic object that captures the information of how far off we are from having $R$ act faithfully on some simple $R$-module. We will now define such an object - the Jacobson radical $J(R)$. The radical is an ideal consisting of those elements which can't be detected by simple modules. Accordingly, it will turn out that $J(R) = 0$ precisely when $R$ has "enough" simple $R$-modules; and $J(R)$ will vanish if there exists a faithful simple $R$-module.

**Definition:** The (Jacobson) **radical** of a ring $R$, denoted $\boldsymbol{J(R)}$ , is the set of those $r \in R$ such that $r \in ann(M)$ for every simple (left) $R$-module $M$; that is,

$$J(R) = \bigcap_{M \text{ simple}} ann(M).$$

If $J(R) = 0$, we say that "$R$ has no radical."

**Remarks:**

1. It is easy to check that $J(R)$ is a two-sided ideal. It is also easy to check that $ann(M)$ is a maximal left ideal for each simple module $M$, and that, conversely, each maximal left ideal $I$ is the annihilator of some simple $R$-module (namely, $R/I$). This is true because, as stated in Proposition 1.1, simple $R$-modules are precisely $R/I$ for maximal left ideals $I$. Thus we see that, alternatively,

$$J(R) = \bigcap_{\substack{\text{max. left} \\ \text{ideals } I}} I$$

   This shows that $J(R)$ can be intrinsically defined. Such a definition is useful in computing the Jacobson radical, as long as we can get sufficient information on the maximal ideals of the ring at hand. This is the case in examples 1, 2, and 4 below. Note that, in particular, $J(R) \neq R$.

2. Some authors say "$R$ is semsimple" when referring to rings with $J(R) = 0$. This is, in general, not the same as our definition of the word; the ring $\mathbf{Z}$, for example, has vanishing radical but is not semisimple. Such people (usually ring-theorists) would say "semisimple with minimum condition" when referring to our definition of semisimple; here "minimum condition" refers to the descending chain condition. Theorem 2.2 will show that their "semisimple with minimum condition" really does coincide with our definition of semisimple.

We now give a few examples where the radical can be computed explicitly. Other examples may be found (and worked out) in the exercises.

**Examples:**

**1.** $J(D) = 0$ for $D$ a division ring, since $D$ has no (nontrivial) maximal left ideals.

**2.** $J(\mathbf{Z}) = \bigcap_{p \text{ prime}} p\mathbf{Z} = 0.$

**3.** $J(\mathbf{Z}/p^n\mathbf{Z})$ is the unique maximal ideal $p\mathbf{Z}/p^n\mathbf{Z}$ of $\mathbf{Z}/p^n\mathbf{Z}$, which is non-trivial for $n \geq 2$. For the proof of this fact, see the discussion after Proposition 2.8.

**4.** $J(\mathcal{M}_n(R)) = \mathcal{M}_n(J(R))$. The proof of this fact is Exercise 16.

It should be noted that many radicals other than $J(R)$ have been constructed, such as the prime radical and the nilradical (which is treated in Exercise 19). These radicals capture other "undesirable" properties of a ring $R$. For an extensive treatment of radicals see M.J. Divinsky, *Rings and Radicals*, and M. Gray, *A Radical Approach to Algebra.*

The radical $J(R)$ is the intersection of all maximal left ideals of $R$. This intersection may be infinite, and it would be nice to know if there is some finite family of maximal left ideals whose intersection is precisely $J(R)$; thus making $J(R)$ easier to deal with. In general, it is not true that such a finite family exists; some sort of "finiteness condition" must be put on the ring. Since the radical involves intersections, one might guess that the appropriate finiteness condition to put on the ring $R$ would be that there are no infinite descending chains; that is, that $R$ is artinian (see Chapter Zero for the definition of artinian ring). This will suffice, as we now show.

**Lemma 2.1** *If $R$ is an artinian ring, there is a finite family $\{L_1, \ldots, L_n\}$ of ideals such that $J(R) = \bigcap_{i=1}^n L_i$.*

**Proof:** If $R$ has no maximal left ideals other than zero then the lemma is trivial, so assume otherwise. Let

$$\mathcal{S} = \{\cap L_i : \{L_i\} \text{ is a finite family of maximal left ideals}\}.$$

By assumption $\mathcal{S}$ is not empty. Since $R$ is artinian, there exists a minimal (with respect to inclusion) element $Q$ of $\mathcal{S}$ (Chapter Zero, Exercise 43). If $I$ is any maximal left ideal, then $I \cap Q \subseteq Q$, so $Q = I \cap Q$ by minimality of $Q$. Thus $Q \subseteq I$ for all maximal left ideals $I$; that is, $Q \subseteq J(R)$. Clearly $J(R) \subseteq Q$, and so $J(R) = Q$, an intersection of finitely many maximal left ideals. □

Although Chapter One gives seven equivalent characterizations of a semisimple ring, it may still be difficult to prove, using only these definitions, that a given ring is semisimple. Perhaps this is because none of these definitions is intrinsic to the ring at hand; each involves different modules associated with the ring. The Jacobson radical is intrinsic, and can be a useful tool in determining if a ring is semisimple. The relationship between the Jacobson radical and semisimplicity is given by the following theorem, which will complete our list of characterizations of semisimple rings given in Theorem 1.18.

**Theorem 2.2** *$R$ is semisimple if and only if $R$ is artinian and $J(R) = 0$.*

**Proof:** Assuming that $R$ is semisimple, Theorem 1.9 shows that $R$ has finite length and is thus artinian. To show that $J(R) = 0$, first note that any matrix ring $\mathcal{M}_n(D)$ over a division ring is simple, so by condition (5) of the Structure Theorem for Simple Artinian Rings, $\mathcal{M}_n(D)$ has a faithful simple module, and hence $J(\mathcal{M}_n(D)) = 0$. Alternatively, note that $\mathcal{M}_n(D)$ has no nontrivial two-sided ideals (Chapter 1, Exercise 5), and since $J(\mathcal{M}_n(D))$ is a two-sided ideal not equal to $\mathcal{M}_n(D)$, $J(\mathcal{M}_n(D)) = 0$. Since $R$ is semisimple, $R$ is a finite product of matrix rings over division rings, each of which has trivial radical. The result follows from the fact that $J(R_1 \times R_2) = J(R_1) \times J(R_2)$ for rings $R_1, R_2$ (see Exercise 5).

Now assume that $R$ is artinian and $J(R) = 0$. By Corollary 1.5, it suffices to show that $R$ embeds as a submodule of some semisimple module. Well, since $R$ is artinian and $J(R) = 0$, there exists, by Lemma 2.1, a finite collection $\{L_i\}$ of maximal left ideals whose intersection is zero. Thus the natural map

$$R \longrightarrow \bigoplus_i R/L_i$$

has zero kernel (note that the image really is a sum since $\{L_i\}$ is finite). Hence $R$ embeds as a submodule of the semisimple module $\bigoplus_i R/L_i$, and is thus (by Corollary 1.5) semisimple. □

This theorem gives us a new way of determining whether a ring is semisimple, at least in the case of artinian rings. It is often easier to compute the radical than to realize one of the seven characterizations given earlier of semisimple rings. Theorem 2.2 may also be viewed as showing that, at least for artinian rings, $J(R)$ is a measure of how far $R$ is from being semisimple.

We now make precise the statement in the beginning discussion of this chapter that the radical "captures an undesirable property". In the case at hand, $J(R)$ consists of elements that are undesirable in the sense that they annihilate every simple $R$-module. Since $J(R)$ consists of all these annihilating elements, the quotient ring $R/J(R)$ should contain no such elements; that is, $R/J(R)$ should have no radical. This idea has an analog in any type of radical we define; namely, if $J$ is some radical (Jacobson, prime, nil, etc.) of $R$, then $R/J$ should have no radical (of that type). Thus, for our study of the Jacobson radical, we give the following

**Corollary 2.3** *$R/J(R)$ has no radical; hence if $R$ is artinian, $R/J(R)$ is semisimple.*

**Proof:** $R/J(R)$ has no radical since simple $R/J(R)$-modules are in one-to-one correspondence with simple $R$-modules. If $R$ is artinian, so is $R/J(R)$, and so $R$ is semisimple by Theorem 2.2. □

Corollary 2.3 is frequently used when proving statements about artinian rings. The typical argument is as follows : If one wishes to prove a certain statement concerning an artinian ring $R$, it suffices to show that the statement holds for $R/J(R)$. Since $R/J(R)$ is artinian and has no radical, it is semisimple and is thus a product of matrix rings over division rings. This often reduces the original question to a question about matrices, where computational techniques may be used. See Chapter Three, Exercise 18 for an example of this kind of argument.

# Properties of the Jacobson Radical

We now explore some of the properties of the Jacobson radical. We also introduce the concept of nilpotence, which will be useful in describing some of these properties and in making computations.

We call $r \in R$ a **nilpotent element** if $r^n = 0$ for some $n$. An ideal $I \subseteq R$ is called a **nilpotent ideal** if $I^n = 0$ for some $n$ (here $I^n$ denotes a product of ideals). Note that this is stronger than saying that all of the elements of $I$ are nilpotent, since $I^n = 0$ says that all $n$-fold products $r_1 r_2 \cdots r_n$ (each $r_i \in I$) are zero. If $R$ is commutative and $I$ is a finitely generated ideal, however, we have : $I$ is nilpotent $\Longleftrightarrow$ all elements of $I$ are nilpotent $\Longleftrightarrow$ $I$ is generated by nilpotent elements.

We shall now show how the radical of a ring may be characterized by the ring's nilpotent ideals.

**Theorem 2.4** *Any nilpotent ideal of a ring $R$ is contained in $J(R)$. If $R$ is artinian, then $J(R)$ is nilpotent and hence is the largest nilpotent ideal of $R$.*

Note that $J(R)$ is not necessarily nilpotent if $R$ is not artinian (see Exercise 20).

**Proof:** Let $I$ be a nilpotent ideal. We must show $IM = 0$ for any simple module $M$. Well, if $IM \neq 0$ then $IM = M$ since $M$ is simple, so $I^2M = IM = M$. Continuing this gives $I^nM = M$; but $I^n = 0$, so $I^nM = 0M = 0$, a contradiction. Thus $I \subseteq J(R)$.

Now assume that $R$ is artinian and let $J = J(R)$. Since $R$ is artinian, the descending chain $J \supseteq J^2 \supseteq \cdots$ must stabilize; that is, $J^n = J^{n+1}$ for some $n$. Let $A = J^n$. If $A = 0$, then $J$ is nilpotent and we are done, so suppose $A \neq 0$. Let $I$ be a left ideal of $R$ which is minimal among left ideals $L$ such that $AL \neq 0$. Such an $I$ exists since $R$ is artinian, and since

the collection of such ideals is not empty; for example, $AJ = A \neq 0$. Now $A(JI) = (AJ)I = AI \neq 0$, so $JI = I$ by the minimality of $I$.

We claim that $I$ is generated by a single element: Since $AI \neq 0$, there exists $x \in I$ such that $Ax \neq 0$. But $Ax \subseteq I$ is a left ideal, and $A \cdot Ax = Ax$, so by minimality of $I$ we have $Ax = I$. In particular, since $x \in I$, there exists $a \in A$ with $ax = x$, and so $(1-a)x=0$. Now if we can prove that $(1-a)$ has a left inverse, then $x = 0$, and so $I = Ax = 0$, hence $AI = 0$, a contradiction. Thus it would be that $A = 0$ and so $J$ is nilpotent.

So now all that is left is to show that $1 - a$ has a left inverse for any $a \in J(R)$. Well, by definition of the radical, $a$ is contained in every maximal left ideal, so clearly $1 - a$ is in no maximal left ideal. Hence $1 - a$ is in no proper left ideal, so $R(1 - a) = R$. In particular, $1 = r(1 - a)$ for some $r \in R$ and we are done. □

For a proof of the second part of Theorem 2.4 which follows the module-theoretic theme of this book, the reader may see Exercise 28. The argument in the last paragraph is a special case of both Proposition 2.8 and Nakayama's Lemma, which we shall see later in the chapter. The type of argument used is a typical application of these results.

**Example:** Theorem 2.4 can be used to calculate the radical of $R = \mathbf{Z}/p^n\mathbf{Z}$, $p$ a prime, as follows. All proper nonzero ideals of $R$ clearly have the form $p^iR, i = 1, \ldots, n$. Clearly every ideal is nilpotent, and $pR$ is the largest (nilpotent) ideal. Hence, by Theorem 2.4, $J(R) = pR$. Note that $J(R) = pR$ is nontrivial for $n \geq 2$.

Theorem 2.2 gives a relationship between semisimplicity and the vanishing of the radical. Combining this with the above description of $J(R)$ as the largest nilpotent ideal of $R$ will give us another method, in terms of nilpotent ideals, of determining if a ring is semisimple. If $R$ is commutative, it will suffice to check whether or not there are any nilpotent elements. Thus we give the following :

**Corollary 2.5** *$R$ is semisimple if and only if $R$ is artinian and has no non-zero nilpotent left ideals. If $R$ is commutative, then $R$ is semisimple if and only if $R$ is artinian and has no nilpotent elements.*

**Proof:** The first part of this corollary is clear from Theorem 2.4. For the commutative case, note that a nilpotent element generates a nilpotent ideal, since $a^n = 0$ if and only if $(Ra)^n = Ra^n = 0$. □

Another application of Theorem 2.4, combined with Theorem 2.2 and Wedderburn's Theorem yields the following corollary.

**Corollary 2.6** *If $R$ is artinian, then $R$ has a nilpotent two-sided ideal $J$ such that $R/J$ is isomorphic to a finite product of matrix rings over division*

*rings, with factors in one-to-one correspondence with isomorphism classes of simple R-modules.*

These two corollaries can be used to show that any artinian ring (with unit) is noetherian. This result is striking because these two concepts have no obvious connection; intuitively, what happens at the "bottom" of a ring shouldn't have much to do with what happens at the "top". The converse, in fact, is not true; for example, $\mathbf{Z}$ is noetherian but not artinian. Note also that the result does not hold for modules: an artinian module need not be noetherian, as is demonstrated by the $\mathbf{Z}$-modules $\mathbf{Z}_{p^\infty}$ (Exercise 42 of Chapter 0). The fact that every artinian ring is noetherian can be quite useful, as we saw in the proof of Corollary 2.6. Thus we give the following:

**Theorem 2.7 (Hopkin's Theorem)** *If $R$ is artinian (with identity) then $R$ is noetherian.*

**Proof:** An outline of the proof, with a few gaps waiting to be filled by an eager reader, can be found in Exercise 31. □

We now give some results that describe $J(R)$ on the level of individual elements. This can be useful in certain cases for computing the radical.

**Proposition 2.8** *$x \in J(R)$ if and only if $1 + ax$ has a left inverse for all $a \in R$.*

**Proof:** If $x \in J(R)$, then $ax \in J(R)$ since $J(R)$ is a two-sided ideal . Thus we have that $ax$ is in every maximal left ideal, so clearly $1 + ax$ is in no maximal left ideal. Hence $1+ax$ is in no proper left ideal, so $R(1+ax) = R$. In particular, $1 = r(1 + ax)$ for some $r \in R$ and we are done.

Conversely, if $x \notin J(R)$, then there exists some maximal left ideal $I$ such that $x \notin I$. So $I + Rx = R$ by maximality of $I$. In particular, $1 = r + ax$ for some $r \in I, a \in R$; that is, $1 - ax = r \in I$ has no left inverse (remember that $br \neq 1$ for any $b \in R$ since $I$ is a proper ideal). □

**Example:** As an application of Proposition 2.8, we compute the radical of a ring that is useful in number theory and topology. The **localization** of $\mathbf{Z}$ at a prime ideal $p$, denoted by $\mathbf{Z}_{(p)}$, is the subring of $\mathbf{Q}$ given by

$$\mathbf{Z}_{(p)} = \{\frac{m}{n} : (p, n) = 1\}.$$

First note that the invertible elements of $\mathbf{Z}_{(p)}$ are precisely those rational numbers with numerator relatively prime to $p$. Hence $1 + (\frac{m}{n})(p\frac{m'}{n'})$ is invertible for all $\frac{m}{n}, \frac{m'}{n'} \in \mathbf{Z}_{(p)}$; hence $p\mathbf{Z}_{(p)} \subseteq J(\mathbf{Z}_{(p)})$. Now if $(m, p) =$

1, then (remember the Euclidean Algorithm) there exist $\alpha, \beta \in \mathbf{Z}$ with $\alpha m + \beta p = 1$. Then $1 - \alpha m = \beta p$ has no inverse in $\mathbf{Z}_{(p)}$, and so $m$ is not contained in the radical. It follows that $\frac{m}{n}$ is not contained in the radical for any $m$ with $(m, p) = 1$, and so $J(\mathbf{Z}_{(p)}) = p\mathbf{Z}_{(p)}$, which is always nontrivial.

We continue with another useful characterization of the Jacobson radical.

**Proposition 2.9** *If $x \in J(R)$ then $1 + x$ is invertible (i.e. has a two-sided inverse). Moreover, $J(R)$ is the largest two-sided ideal with this property.*

**Proof:** We already know by Proposition 2.8 that $1 + x$ has a left inverse, call it $z$. Clearly $z - 1 \in J(R)$, so $z = 1 + y$ for some $y \in J(R)$. Again by Proposition 2.8, $1 + y$ has a left inverse; but $1 + y$ also has a right inverse, namely $1 + x$. Thus $1 + x$ and $1 + y$ are (two-sided) inverses of each other.

Now if $I$ is any two-sided ideal with this property, then $1 + ax$ is invertible for all $a \in R, x \in I$, so by the Proposition 2.8 we have $x \in J(R)$. Thus $I \subseteq J(R)$. □

Thus far we have dealt with what should really be called the "left radical" of $R$. We could also define a "right radical" of $R$ to be the intersection of all maximal right ideals of $R$, and by the same technique used in proving Proposition 2.8, we can show that

$x \in J(R)$ *if and only if* $1 + xb$ *has a right inverse for all* $b \in R$.

But Proposition 2.9 gives a *symmetric* characterization of the radical, so the left radical and right radical must coincide. We state this formally as

**Corollary 2.10** $J(R) \approx J(R^\circ)$.

We conclude this section with one more characterization of the Jacobson radical in the hope that the many different views we have taken of this creature will help to give the reader a good picture and intuition for it.

An element $r$ of a ring $R$ is called a **non-generator** of $R$ if, whenever $S$ is a subset of $R$ such that $S \cup \{r\}$ generates $R$, then $S$ alone generates $R$. First note that every element $r$ of $J(R)$ is a non-generator, for if $\{x_1, \ldots, x_n, r\}$ generates $R$, then in particular

$$c_1 x_1 + \cdots + c_n x_n + c_{n+1} r = 1$$

for some $c_1, \ldots, c_{n+1} \in R$. But $c_1 x_1 + \cdots + c_n x_n = 1 - c_{n+1} r$ has a left inverse by Proposition 2.8, so in fact $\{x_1, \ldots, x_n\}$ generates $R$. Conversely, if $r \in R$ is a non-generator, then $r$ must be contained in every maximal left ideal $I$, for otherwise $I \cup \{r\}$ would generate $R$ by maximality of $I$. Hence $r \in J(R)$. So we now have another characterization of the radical :

$J(R)$ is the set of non-generators of $R$.

In group theory, there is an analogous definition of a non-generating element. In this case one studies the set of non-generators of a group $G$, which is called the Frattini subgroup of $G$. The Frattini subgroup plays a role in group theory which is analogous to that of the Jacobson radical in ring theory.

## Nakayama's Lemma and Applications

We now give a lemma that is simple but extremely useful in a variety of situations. This lemma, called Nakayama's Lemma, often reduces a local question to that of a field, where techniques from linear algebra can be applied. We shall make this more precise later.

**Lemma 2.11 (Nakayama's Lemma)** *If $M$ is a finitely generated $R$-module such that $J(R)M = M$, then $M = 0$.*

**Proof:** Since $J(R)$ annihilates every simple module, we have $J(R)(M/M')=0$ for all maximal submodules $M'$ of $M$, and so $J(R)M \subseteq M'$. If $M$ is finitely generated and non-zero, then such an $M'$ exists by Zorn's Lemma, and hence $J(R)M \neq M$ since $M'$ is proper, contradicting the given. Thus $M$ must be 0 and we are done. □

**Remarks:**

**1.** A trivial, alternate proof of Nakayama's Lemma may be given when $J(R)$ is nilpotent, say $J(R)^n = 0$, for then $M = J(R)M = J(R)^2(M) = \cdots = J(R)^n M = 0$. In particular, if $R$ is artinian then $J(R)$ is nilpotent (Theorem 2.4), and so this proof will work.

**2.** Even if $J(R)M = M$ holds, the conclusion of Nakayama's Lemma can fail if $M$ is not finitely generated (see Exercise 35).

Nakayama's Lemma may be stated in several ways. We now give two equivalent reformulations of Nakayama's Lemma that will be useful for applications.

**Equivalent Formulations of Nakayama's Lemma**

**1.** Let $M$ be a finitely generated $R$-module. If $N$ is a submodule of $M$, then $N + J(R)M = M$ if and only if $N = M$.

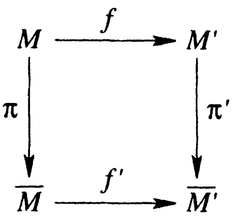
**2.** Recall that if $M$ is an $R$-module and $I$ is a two-sided ideal of $R$, then $IM$ is a submodule of $M$, and the module $M/IM$ is annihilated

by $I$. Thus $M/IM$ may be regarded in a natural way as a module over $R/I$. For $I = J(R)$, $\overline{M} = M/J(R)M$ can be considered as a module over $\overline{R} = R/J(R)$. Supposing further that $M$ is finitely generated, Nakayama's Lemma is then equivalent to the following: $M = 0$ if and only if $\overline{M} = 0$.

It is not difficult to check that these two statements are equivalent to Lemma 2.11; the reader is encouraged to do so.

We now give two applications of Nakayama's Lemma; others will be given throughout the exercises (although the reader may not always be told when the lemma should be applied!). Using the forms of the lemma stated above, one can often reduce questions about $M$ to questions about $\overline{M}$, where, as above, $\overline{M} = M/J(R)M$ is considered as a module over $\overline{R} = R/J(R)$. $\overline{M}$ is easier to work with since $\overline{R}$ is a 'nicer' ring than $R$. For example, $\overline{R}$ has no radical, and is thus semisimple if $R$ is artinian. Another example arises when $R$ is a local ring (defined in the exercises), in which case $\overline{R}$ is a field, and so linear algebra may be used to determine the answers to questions about $\overline{M}$. This philosophy is demonstrated by the following two corollaries.

Suppose $f : M \longrightarrow M'$ is a homomorphism of a module $M$ into a finitely generated module $M'$. Since $f(IM) \subseteq IM'$ for any ideal $I$ of $R$, we have in particular that $f(J(R)M) \subseteq J(R)M'$. Thus $f$ induces a homomorphism $\overline{f} : \overline{M} \longrightarrow \overline{M}'$ making the following diagram commute :




Here $\pi : M \longrightarrow \overline{M} = M/J(R)M$ and $\pi' : M' \longrightarrow \overline{M}' = M'/J(R)M'$ are the natural quotient maps.

**Corollary 2.12** *Let $f : M \longrightarrow M'$ be a homomorphism with $M$ finitely generated such that $\overline{f} : \overline{M} \longrightarrow \overline{M'}$ is surjective. Then $f$ is surjective.*

**Proof:** Apply (1) above with $N = image(f)$. □

**Corollary 2.13** *Let $M$ be a finitely generated $R$-module, and let $\{x_i\}$ be a collection of elements of $M$. Then $\{x_i\}$ generates $M$ if and only if $\{\overline{x}_i\}$ generates $\overline{M}$.*

**Proof:** Apply the previous corollary with $M$ the submodule generated by $\{x_i\}$. □

Although seemingly trivial, these corollaries, along with Nakayama's Lemma, are extremely useful in proofs. Several applications will be given in the exercises, both in a special section and scattered throughout.

# Summary

Throughout this Chapter we have seen several different ways of looking at the Jacobson radical $J(R)$. Since it is useful to keep all of these characterizations in mind when trying to compute the radical of a given ring, we now give a summary of equivalent definitions of $J(R)$.

**Equivalent Definitions of the Jacobson Radical of a Ring $R$**

(1) $J(R) = \bigcap_{\substack{\text{simple left} \\ \text{modules } M}} ann(M) = \bigcap_{\substack{\text{simple right} \\ \text{modules } M}} ann(M)$.

(2) $J(R) = \bigcap_{\substack{\text{max. left} \\ \text{ideals } I}} I = \bigcap_{\substack{\text{max. right} \\ \text{ideals } I}} I$.

(3) $J(R) = \{x \in R : 1 + ax$ has a left inverse for all $a \in R\}$.

(4) $J(R) = \{x \in R : 1 + xb$ has a right inverse for all $b \in R\}$.

(5) $J(R) = \{x \in R : 1 + axb$ has a (two-sided) inverse for all $a, b \in R\}$.

(6) $J(R)$ is the largest two-sided ideal of $R$ with the property that $1 + x$ has a two-sided inverse for every element $x$ of the ideal.

(7) $J(R)$ is the set of non-generators of $R$.

The equivalence of all of these definitions, except for (5), was discussed in the text. It is easy to check that (5) is equivalent to both (3) and (4), and thus to the rest of the characterizations. When computing the radical of a given ring, the trick is to choose the proper characterization ((1)-(7)) of $J(R)$.

For artinian rings, we may further characterize $J(R)$ as the largest nilpotent ideal of $R$. Also for artinian rings, semisimplicity of $R$ is equivalent to the vanishing of $J(R)$. In this sense the radical of an artinian ring $R$ measures how far $R$ is from being semisimple.

# Exercises

## Properties of the Radical

1. Show that if $f : R \longrightarrow S$ is a ring surjection, then $f(J(R)) \subseteq J(S)$.

Show by example that this inclusion need not be an equality. What happens if $f$ is not surjective?

2. Let $I$ be an ideal of a ring $R$. Show that if $J(R/I) = 0$, then $I \supseteq J(R)$. In particular, if $I \subseteq J(R)$ and $J(R/I) = 0$, then $I = J(R)$.

3. Let $R$ be a ring and suppose $v \in R$ is invertible in $R/J(R)$. Prove that $v$ is invertible in $R$.

4. Let $R$ be a ring, and let $M$ be an $R$-module. Prove that $M$ is semisimple if and only if $ann(x)$ is the intersection of finitely many maximal left ideals of $R$ for all $x \in M, x \neq 0$. [Hint: Try it first for $M$ cyclic.]

5. If $\{R_i\}_{i\in I}$ is a family of rings, show that $J(\prod_{i\in I} R_i) = \prod_{i\in I} J(R_i)$.

6. Let $S$ be a ring and let $R$ be a subring of $S$. Assume that $S$ is finitely generated as a left $R$-module, and that $SJ(R) = J(R)S$ (this is automatic, for example, if $R$ is central in $S$). Prove that $J(R) \subseteq J(S)$.

7. (a) Let $e$ be an idempotent in a ring $R$; i.e., $e^2 = e$. Prove that $eJ(R)e = J(eRe)$.

   (b) Show that if $e \in J(R)$ is an idempotent, then $e = 0$. More generally, show that if $x^n = x$ for some $n \geq 2$ and $x \in J(R)$, then $x = 0$.

8. If $I$ is a two-sided ideal in a ring $R$, show that $J(R/I) \supseteq (I+J(R))/I$. If $I \subseteq J(R)$, show that equality holds, and that equality need not hold otherwise.

9. Remember that $J(R)$ is the intersection of all maximal left (or right) ideals of $R$. This problem constructs a ring $R$ such that $J(R)$ is *not* the intersection of maximal *two-sided* ideals of $R$. Let $K$ be a field of characteristic 0, $\sigma$ an automorphism of $K$ of infinite order, and let $R$ be the ring consisting of all (non-commuting) polynomials $f(x) = a_0 + a_1x + \cdots + a_nx^n$ with $a_i \in K$, but with multiplication defined by the rule :

$$(ax^m)(bx^n) = a\sigma^m(b)x^{m+n} \qquad \text{for all } a, b \in K$$

   This ring is usually called a **twisted polynomial ring** . Prove that:

   (a) A subset of $R$ is a non-zero two-sided ideal of $R$ if and only if it has the form $Rx^n$ for some $n \geq 0$.

   (b) $Rx$ is the unique maximal two-sided ideal of $R$, and $R/Rx \approx K$ as rings.

   (c) $J(R) = 0$. [Hint: Start by looking for some maximal left ideals of $R$, or perhaps some simple left $R$-modules.]

10. Do a similar construction as in Exercise 9 for Laurent polynomials, and show that this provides an example of a simple ring with no zero divisors which is not a division ring.

11. (a) Let $R$ be a semisimple artinian ring, and let $M$ be a faithful left $R$-module. Prove that, if $R$ is also commutative, then $M \approx R \oplus N$ for some $R$-module $N$. Give an example to show that this is not true in general if $R$ is not commutative.

    (b) Prove that $J(R) = 0$ if and only if there is a faithful semisimple $R$-module.

    (c) Assume that $R$ has finitely many maximal left ideals and that $J(R) = 0$. Prove that $R \approx R_1 \times \cdots \times R_n$, where, for each $1 \leq i \leq n$, either $R_i$ is a division ring or $R_i \approx \mathcal{M}_{n_i}(k_i)$ with $k_i$ a finite field. [Hint: First show that $R$ is semisimple artinian.]

    (d) Why is this one problem instead of three?

### Computing $J(R)$

12. (a) Compute $J(R)$ in the following cases :

    (i) $R = \mathbf{Z}/8\mathbf{Z}$.

    (ii) $R = \mathbf{Z}/60\mathbf{Z}$.

    (iii) $R = \mathbf{Q}[x]/(x^3 - 5x)$.

    (iv) $R = \mathbf{Q}[[x]]$, the ring of formal power series.

    (v) $R = \mathbf{F}_p[\mathbf{Z}/p\mathbf{Z}]$, the group ring over the field $F_p$ with $p$ elements ($p$ a prime).

    (vi) $R$ is a principal ideal domain which is not a field. [Hint: The answers are different depending on whether $R$ has finitely or infinitely many primes.]

    (vii) $R = S[x]$ with $S$ a (commutative) integral domain.

    (b) Which of the above are semisimple?

    (c) Compute the radical of $\mathbf{Z}/n\mathbf{Z}$. For which $n$ is $\mathbf{Z}/n\mathbf{Z}$ semisimple?

13. Let $R$ be a principal ideal domain. Let $a$ be a nonzero element of $R$, and write $S = R/(a)$. Describe $S$ in terms of the factorization of $a$. Compute $J(S)$. Compute $S/J(S)$. Give an explicit description of all finitely generated projective $S$-modules. List (up to isomorphism) all simple $S$-modules.

14. Consider the ring of all continuous real-valued functions on $[0, 1]$. What is the radical of this ring?

15. Let $k$ be a field. For each $k$-algebra $A$ given below, do the following: Find $J(A)$; find all simple left $A$-modules (up to isomorphism); and express $J(A)^i/J(A)^{i+1}$ as a direct sum of simple $A$-modules for all $i \geq 0$.

(a) $A = k[x]/(x^n)$, $n \geq 0$.

(b) $A =$ the set of $2 \times 2$ upper triangular matrices with entries in $k$.

(c) $A = \mathcal{M}_2(k)$ as a $k$-space, but with multiplication defined by the formula

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa' & ab' + bd' \\ ca' + dc' & dd' \end{bmatrix}$$

(d) The ring of matrices of the form

$$\begin{pmatrix} r & m \\ 0 & s \end{pmatrix}$$

where $r \in R$, $s \in S$ and $m \in M$ for rings $R$ and $S$ and an $R$-$S$ bimodule $M$.

16. If $R$ is a ring, show that $J(\mathcal{M}_n(R)) = \mathcal{M}_n(J(R))$. What does this say about the radical of a matrix ring over a division ring? About the radical of a semisimple ring?

17. (a) Find $J(\mathcal{T}_n(D))$, where $\mathcal{T}_n(D)$ is the ring of all upper triangular $n \times n$ matrices over a division ring $D$.

(b) Show that $\mathcal{T}_n(D)/J(\mathcal{T}_n(D))$ is isomorphic to the direct product $D \times D \times \cdots \times D$ ($n$ factors).

(c) If $S$ is a subring of $\mathcal{T}_n(D)$ such that $S \supseteq D$, show that $J(S) = S \cap J(\mathcal{T}_n(D))$.

### Nilpotence

18. An ideal $I$ (left, right, or two-sided) is called a **nil ideal** if all its elements are nilpotent. Prove that any nil ideal (left or right) of a ring $R$ is contained in $J(R)$.

19. (a) Let $I$ and $J$ be two-sided nil ideals of $R$. Prove that $I + J$ is a nil ideal.

(b) Let $Nil(R)$ denote the two-sided ideal generated by all two-sided nil ideals of $R$. $Nil(R)$ is called the **nilradical** of $R$. Prove that

$Nil(R)$ is a nil ideal of $R$ and that $R/Nil(R)$ possesses no non-zero nil ideals; that is, $Nil(R/Nil(R)) = 0$.

(c) Prove that $Nil(R) \subseteq J(R)$.

(d) Compute $Nil(R)$ for all of the rings discussed so far in this chapter. Which one of these gives an example to show that equality does not necessarily hold in part (c)?

(e) Show that for a commutative ring $R$, $Nil(R)$ is the intersection of all prime ideals of $R$ (recall that an ideal $P \neq R$ is **prime** if, for all ideals $A, B$ of $R$, $AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$).

(f) Show that for a commutative ring $R$, $J(R[x]) = Nil(R)[x]$.

20. This exercise provides two examples of rings with ideals that are nil but not nilpotent.

(a) Let $R$ be the ring of infinite matrices (with entries in a field) whose rows are eventually zero; that is, if $[a_{ij}] \in R$, then there is an $n$ with $a_{ij} = 0$ for all $j > n$. Let $S$ be the subring of $R$ consisting of matrices with zeros below the main diagonal. Show that $J(S)$ is the set of matrices that have zeros on the main diagonal (i.e., the set of $[a_{ij}]$ with $a_{ii} = 0$). Show that $J(S)$ is nil but not nilpotent. This also gives an example of a ring whose radical is not nilpotent.

(b) Let $R = k[x_1, x_2, \ldots]$ be the ring of polynomials with commuting indeterminants $x_1, x_2, \ldots$. Let $I$ be the ideal of $R$ generated by $\{x_1^2, x_2^2, \ldots\}$. Prove that $R/I$ has nil ideals that are not nilpotent.

21. (a) Show that in non-commutative rings, nilpotent elements do not necessarily generate nilpotent ideals. [Hint : Look at $\mathcal{M}_n(\mathbf{Q})$.] Show that a finite number of nilpotent elements do generate nilpotent ideals in commutative rings.

(b) For $D$ a division ring, show that $\mathcal{M}_n(D)$ contains no two-sided nilpotent ideals. Hence a semisimple ring contains no two-sided nilpotent ideals.

(c) Show that the ring $\mathcal{T}_n(D)$ is not a semisimple ring for $n \geq 2$.

(d) Show that any non-zero left ideal of $\mathcal{M}_n(D)$ contains a non-zero idempotent. Hence $\mathcal{M}_n(D)$ contains no left nil ideals. Draw the same conclusion for a semisimple ring.

**Remark:** It is easy to see what the left ideals of $\mathcal{M}_n(D)$ look like. Think about this, especially in connection with Wedderburn's Theorem.

22. Let $M$ be an $R$-module of finite length. Show that $J(End_R(M))$ is nilpotent.

23. (a) Give another proof of the converse of Maschke's Theorem by exhibiting, if $|G|$ is not invertible in $k$, a nil ideal of $k[G]$.

(b) For fun, try to solve the following open questions : If $G$ is an infinite torsion-free group, can $k[G]$ contain idempotents? Zero-divisors? Nilpotent elements? Non-trivial units? What are the answers to these question if the group has torsion (this is not hard)?

The answers to these questions for certain cases are known. See Zalesskii and Mikhalev's article "Group Rings", as well as Passman's survey "Advances in Group Rings".

24. Let $R$ be an artinian ring and let $G$ be a finite group. Show that $R[G]$ is semisimple if and only if $R$ is semisimple and $|G|$ is invertible in $R$.

25. (a) Let $I$ be a non-zero ideal of $R[x]$, and let $p(x) \in R[x]$ be a non-zero polynomial of least degree in $I$ with leading coefficient $a$. Show that if $f(x) \in R[x]$ and $a^m f(x) = 0$, then $a^{m-1}p(x)f(x) = 0$.

(b) Show that if a ring $R$ has no non-zero nil ideals (in particular, if $R$ is semisimple), then $R[x]$ has zero Jacobson radical . [Hint: Let $M$ be the set of non-zero polynomials of least degree in $J(R[x])$. Let $N$ be the set consisting of 0 and the leading coefficients of polynomials in $M$. Use part (a) to show that $N$ is a nil ideal of $R$, whence $J(R[x]) = 0$.]

(c) Show that there exists a ring $R$ such that $R[x]$ has zero Jacobson radical but $R$ does not. [Hint: Consider $R = F[[x]]$, $F$ a field.]

26. Give another proof of the part of Corollary 2.5 that says: If $R$ is an artinian ring and has no non-zero nilpotent left ideals, then $R$ is semisimple. Proceed as follows:

(a) Choose a minimal non-zero left ideal $L$. Show that $L^2 = L$. Fix $x \in L$ with $Lx = L$, and choose $e \in L$ such that $ex = x$. Show that $e^2 = e$ and conclude that $Re = L$ is a simple, idempotent-generated left ideal. Decompose $R$ as a left $R$-module as $R = Re \oplus L_1$, where $L_1 = \{y - ye | y \in R\}$ and note that $L_1 e = 0$.

(b) Assume by induction that $R$ has been decomposed as

$$R = Re_1 \oplus \cdots \oplus Re_n \oplus L_n$$

with $Re_i$ simple and $e_1, e_2, \ldots, e_n$ an orthogonal family of idempotents such that $L_n e_i = 0$ for all $i$. If $L_n \neq 0$, as in part (a), show that there is an $e' \in L_n$ with $Re'$ a simple left ideal, $L_n = Re' \oplus L_{n+1}$, $L_{n+1}e' = 0$. Clearly $e'e_i = 0$ for all $i$, but unfortunately the product in the other order is not necessarily zero. Replace $e'$ by $e_{n+1} = e' - ee'$, where $e = e_1 + \cdots + e_n$. Show that everything works now.

(c) Use the finiteness hypothesis on $R$ to conclude that this process must terminate and hence $R$ can be written as a direct sum of simple left ideals.

(d) In the preceding theorem it is not necessary to assume that $R$ has an identity element. Show that $e = e_1 + \cdots + e_n$ must be the identity element of $R$ in case $R$ is written as above with precisely $n$ summands, and that these are all of the corresponding idempotents. Check that $re = r$ for all $r \in R$. Why must $er = r$ as well? [Hint: Show $s(er - r) = 0$ for all $r, s \in R$.]

27. Part (a) of Exercise 26 shows that in an artinian ring which has no non-zero nilpotent left ideals, any minimal left ideal is generated by an idempotent. Show that, in fact, *every* left ideal of such a ring is generated by an idempotent.

28. Give another proof of the second part of Theorem 2.4 by finishing the following idea : In the terminology of the proof of Theorem 2.4, let $L = \{m \in I : mA = 0\}$. Check that $L$ is an ideal and that $I/L$ is simple. Show that this implies $AJI = 0$ and obtain a contradiction.

29. Prove that if $R$ is an artinian ring and $L$ is a non-nilpotent left ideal of $R$, , then there is an element $y \in L$ such that $y^n \neq 0$ for all $n$. Proceed as follows :

    (a) Find $L_0 \subseteq L$ with $L_0 \neq 0$ and $L_0^2 = L_0$.

    (b) Show that there exists a non-zero left ideal $M$ which is minimal with respect to the properties (i) $L_0M \neq 0$, (ii) $M \subseteq L_0$.

    (c) Show that there exists a non-zero $x \in M$ with $L_0x = M$.

    (d) As $x \in M$ there is a $y \in L_0$ with $yx = x$. Show that this $y$ works.

30. (a) Show that if $R$ is artinian, then a left ideal is nilpotent if and only if it is nil (i.e., every element is nilpotent). Exercise 20 shows that this is not necessarily true if $R$ is not artinian.

    (b) Show that in any artinian ring, maximal nilpotent left ideals exist.

    (c) Show that in any ring, the sum of two nilpotent left ideals is again nilpotent.

    (d) Show that if $R$ is artinian, then there is a unique maximal nilpotent left ideal $J$ containing all nilpotent left ideals.

    (e) If $L$ is a nilpotent left ideal of $R$, show that $Lx$ is also nilpotent for any $x \in R$. Conclude that $J$ of part (d) is a two-sided ideal.

    (f) If $R$ is artinian, show that $R/J$ has no non-zero nilpotent left ideals. Conclude that $R/J$ is semisimple. Conclude that the ideal $J = J(R)$ is nilpotent in case $R$ is artinian, as asserted in Theorem 2.4.

### Hopkin's Theorem

31. (a) Let $R$ be an artinian ring and let $J$ denote its Jacobson radical (which is nilpotent by the Exercise 30 or Theorem 2.4). As $R/J$ is semisimple by Corollary 2.3, each of its modules are sums of simple modules. Now $J^i/J^{i+1}$ is an $R/J$-module. Show that it must be a sum of a finite number of simple modules. Thus the chain $0 = J^n \subseteq J^{n-1} \subseteq \cdots \subseteq J \subseteq R$ can be refined to a composition series for $R$. Conclude that $R$ satisfies the ACC (i.e., is noetherian). You have just proved Hopkin's Theorem (Theorem 2.7); namely :

    *If $R$ is an artinian ring with an identity element, then $R$ is noetherian.*

    (b) Give an example to show that Hopkin's Theorem is false if $R$ is not required to have an identity element. [Hint : Try a ring with trivial multiplication.]

### Jordan Form and Another Proof of Maschke's Theorem

32. (Compare this exercise with Chapter 1, Exercise 27.) Let $K$ be a field and let $G$ be a finite group such that the characteristic of $K$ does not divide the order of $G$. Let $n = |G|$. There is a one-to-one ring homomorphism

$$K[G] \longrightarrow \mathcal{M}_n(K) \approx End_K(K[G])$$

given by sending $v \in K[G]$ to the function 'left multiplication by $v$', and then taking the matrix of this linear transformation with respect to the basis $\{g \in G\}$ of $K[G]$ over $K$. This homomorphism is called the **left regular representation** of $G$. By considering the dimension, $K[G]$ is certainly artinian. Show that $K[G]$ has no nilpotent left ideals as follows: Suppose $I$ is a nilpotent left ideal. If $x = \sum_{g \in G} a_g g \in I$ is a non-zero nilpotent element, show that we can assume that $a_1 \neq 0$. For $z \in K[G]$, let $L_z$ denote left multiplication by $z$. What is $Tr(L_g)$ for $g \neq 1$? (Here $Tr(L_g)$ is the **trace** of the linear tranformation $L_g$; i.e., the sum of the elements on the diagonal of the matrix representing $L_g$ in the given basis.) What is $Tr(L_1)$? What must $Tr(x)$ be? Compute in two different ways, once from the hypothesis on $x$ and once from the formulas for $Tr(L_g)$. This proves, using Corollary 2.5, that $K[G]$ is semisimple, which is the statement of Maschke's Theorem.

**Remark:** You have just computed the "character of the regular representation": a **representation** of $G$ is a map $G \xrightarrow{\rho} GL_m(K)$ for

some $m$; in this case, the map $\rho$ is just $g \mapsto$ [matrix of $L_g$], and $m = n$. The **character** of a representation is the function $\mathcal{X} : G \longrightarrow K$ given by $\mathcal{X}(g) = Tr(\rho(g))$. Character theory is a fruitful way of studying finite groups. See Chapter 6 for more details.

33. If you have forgotten about Jordan canonical form, this is a good time to review. In fact, prove the following: The Jordan form of a matrix $A$ is diagonal if and only if $\frac{\mathbf{C}[x]}{(f)}$ ($f$ the minimal polynomial of $A$) is semisimple.

### More on Nakayama's Lemma

34. Show that the two equivalent formulations of Nakayama's Lemma given on page 65 are actually equivalent to Nakayama's Lemma.

35. (a) Show that, even if $J(R)M = M$, the conclusion of Nakayama's Lemma can fail if $M$ is not finitely generated.

    (b) Show that, in fact, there even exist rings with idempotent radical (i.e., with radical $J = J(R)$ such that $J^2 = J$). [Hint: Consider the quotient of a polynomial ring in infinitely many variables by an appropriate ideal.]

36. Give an another proof of Nakayama's Lemma as follows: Let $x_1, \ldots, x_m$ be a generating set for $M$ with a minimal number of elements. Show that if $M \neq 0$ and $J(R)M = M$, then a smaller generating set exists, thus giving a contradiction.

37. Let $P, Q$ be finitely generated projective $R$-modules, and let $I$ be a two-sided ideal of $R$ such that $I \subseteq J(R)$. Prove that $P/IP \approx Q/IQ$ if and only if $P \approx Q$. This is useful in Algebraic K-Theory.

38. (a) Let $I$ be a two-sided ideal of $R$ contained in $J(R)$. Prove that the canonical homomorphism $R^* \longrightarrow (R/I)^*$ is surjective, where $R^*$ denotes the multiplicative group of invertible elements of $R$.

    (b) Let $I$ be as in part (a). Prove that the canonical homomorphism $GL_n(R) \longrightarrow GL_n(R/I)$ is surjective.

### Local Rings

39. If $R$ is a ring such that the sum of any two non-units is again a non-unit, then show that the collection of non-units is a two-sided ideal of $R$. Call it $I$. Show that this two-sided ideal $I$ is in fact the radical of $R$. Further show that $R/I$ is a division ring. A ring such that $R/J(R)$ is a division ring is called a **local ring**.

40. (a) Remember that the localization of $\mathbf{Z}$ at a prime $p$ is $\mathbf{Z}_{(p)} = \{\frac{m}{n} \in \mathbf{Q} : (p, n) = 1\}$. Show that $\mathbf{Z}_{(p)}$ is a local ring.

(b) Show that, for a field $F$, the ring of formal power series in several variables $F[[x_1, \ldots, x_n]]$ is a local ring.

(c) The **p-adic integers** $\hat{\mathbf{Z}}_p$ can be described as the ring consisting of infinite sequences of integers $(a_1, a_2, \ldots)$, where $0 \leq a_i < p^i$ for all $i$, and $a_k \equiv a_l (mod\, p^k)$ for $k \leq l$. Addition and multiplication of such series is component-wise (mod $p$ to the power of the component). Equivalently, elements $\hat{\mathbf{Z}}_p$ may be taken to be formal power series

$$r_0 + r_1 p + r_2 p^2 + \cdots$$

where $0 \leq r_i < p$, with addition and multiplication as in standard power series, but with "carrying".

Show that $\hat{\mathbf{Z}}_p$ is a local ring. More generally, show that the completion of a ring at a prime ideal is a local ring (for the definitions, see Atiyah-MacDonald, *Introduction to Commutative Algebra*).

41. If $R$ is a local ring, then $R$ has a unique maximal two-sided ideal $I$ (the set of non-units) such that $R/I$ is a division ring. Show that the converse is not true; that is, find a ring $R$ with a unique maximal two-sided ideal $I$, such that $R/I$ is a division ring but $R$ is not local. [Hint: Look at the endomorphism ring of an infinite dimensional vector space and the two-sided ideal of finite rank operators.]

42. Show that $R/I^k$ is a local ring for $R$ a commutative ring and $I$ a maximal ideal. Why is $I/I^k$ the radical of $R/I^k$ ? (cf. example 3 on page 59.)

43. Let $L_n(k)$ denote the ring of upper triangular matrices contained in $\mathcal{M}_n(k)$ for which all of the entries on the diagonal are equal. Compute the radical of this ring. Show that the ring is a noncommutative local ring and compute the residue division ring (i.e. $R/J(R)$).

44. Let $R$ be a local ring. For $A \in \mathcal{M}_n(R)$, let $\overline{A}$ denote the image of $A$ under the canonical homomorphism $\mathcal{M}_n(R) \longrightarrow \mathcal{M}_n(R/J(R))$ induced by $R \longrightarrow R/J(R)$. Show that $A$ is invertible if and only if $\overline{A}$ is invertible.

45. Let $p$ be prime and $k$ be any positive integer. Check that the sequence

$$1 \longrightarrow I + \mathcal{M}_n(p\mathbf{Z}/p^k\mathbf{Z}) \longrightarrow GL_n(\mathbf{Z}/p^k\mathbf{Z}) \longrightarrow GL_n(\mathbf{Z}/p\mathbf{Z}) \longrightarrow 1$$

is exact. Use this to show that the order of $GL_n(\mathbf{Z}/p^k\mathbf{Z})$ is $(p^n - 1)(p^n - p)\cdots(p^n - p^{n-1})(p^{k-1})^{n^2}$. [Hint: It is not hard to compute the orders of the second and fourth terms of the exact sequence.]

46. Let $R$ be an artinian ring. Prove that :

(a) $J(R)^s/J(R)^{s+1}$ is a finitely generated left $R$-module for all $s \geq 0$.

(b) $R$ is a local ring if and only if $R$ possesses no idempotents other than 0 and 1. [Hint: Show that idempotents in $R/J(R)$ can be lifted to idempotents in $R$.]

47. (a) A left $R$-module $M$ is called **indecomposable** if, whenever $M = M_1 \oplus M_2$, then $M_1 = 0$ or $M_2 = 0$. Prove that, if $End_R(M)$ is a local ring, then $M$ is indecomposable.

(b) Let $R$ be a finite dimensional $k$-algebra, $k$ a field, and let $M$ be an indecomposable finitely generated $R$-module. Prove that $End_R(M)$ is a local ring.

48. Let $R$ be a local ring and let $P$ be a finitely generated projective $R$-module. Show that $P$ is actually a free $R$-module as follows : For $J$ the radical of $R$, write $\overline{R}$ for $R/J$ and $\overline{P}$ for $P/JP$. By Nakayama's Lemma, choose a finite set $\{x_i\}$ in $P$ so that their images $\{\overline{x}_i\} \in \overline{P}$ form a basis over $\overline{R}$ and have the further property that the $\{x_i\}$ generate $P$. Let $F$ be a free $R$-module with the same number of generators as you have found for $P$. Map it in the obvious way onto $P$. Show that this map is an isomorphism.

**Remark:** Kaplansky has shown that any projective module over a local ring is free; finite-generation is not necessary. See Kaplansky, "Projective Modules", *Math. Ann.*, 68 (1958), pp. 372-377.

49. Let $G$ be a finite $p$-group for $p$ prime and let $k$ be a field of characteristic $p > 0$. Part (b) will show that $k[G]$ is a local ring. But first:

(a) Show that $k[G]$ has a unique simple module given by the map $k[G] \longrightarrow k$ which is determined by $g \mapsto 1$; this map is usually called the **augmentation map** of $k[G]$. [Hint: Let $S$ be a simple $k[G]$-module and let $A$ be a finite additive subgroup of $S$ which is carried into itself by the action of $G$ (e.g., for $s \in S$ take the additive subgroup generated by $\{gs : g \in G\}$). Note that $pA = 0$. Using the action of $G$ on $A$ by multiplication, apply the fixed point theorem for $p$-groups (see Jacobson, *Basic Algebra I*) and conclude that $A$ contains a nonzero subgroup $A_0$ which is fixed by $G$. Now consider the submodule of $S$ generated by $A_0$.]

(b) Conclude that the augmentation ideal (the kernel of the augmentation map) is the Jacobson radical of $k[G]$ and hence $k[G]$ is a local ring.

(c) A further observation: Let $L$ be any non-zero left ideal of $k[G]$. Show that $N_G \in L$ (remember that $N_G$, the so-called norm element of $k[G]$, is defined to be $\sum_{g \in G} g$). Hence $k[G]$ has a unique non-zero minimal ideal (left or two-sided).

(d) Give an integer large enough so that the radical raised to that power is zero.

### The Radical of a Module

The Jacobson radical of a module is defined in a way analogous to that of the radical of a ring : The **radical** of an $R$-module $M$ is the intersection of the maximal submodules of $M$, and is denoted by $J(M)$. It is easy to see that $J(R)$ is the same whether $R$ is considered as a ring or as an $R$-module, since maximal submodules are precisely the maximal left ideals. Thus we may use the notation $J(R)$ unambiguously.

50. Let $R$ be a ring and $M$ be an $R$-module. Show that $M$ is semi-simple of finite length if and only if $M$ is artinian and $J(M) = 0$. Note that this generalizes Theorem 2.2.

51. Prove the following facts about $J(M)$, each of which has its ring theoretic analog (which are in previous exercises):

    (a) If $M$ is a finitely generated $R$-module, then $J(M) \neq M$.

    (b) If $f : M \longrightarrow N$ is a homomorphism of modules, then $f(J(M)) \subseteq J(N)$.

    (c) If $N$ is a submodule of $M$, then $J(N) \subseteq J(M)$. Further, $J(M/N) \supseteq \frac{J(M)+N}{N}$.

    (d) If $N$ is a submodule of $M$ such that $J(M/N) = 0$, then $N \supseteq J(M)$. In particular, if $N$ is a submodule of $M$ such that $N \subseteq J(M)$ and $J(M/N) = 0$, then $N = J(M)$.

    (e) Using the previous parts of this exercise, prove

    **Proposition 2.14 (Nakayama's Lemma for Modules)** *If $N$ is a submodule of $M$ with $N + J(M) = M$, then $M = N$.*

52. (a) Prove that, if $\{M_i\}$ is a family of $R$-modules, then $J(\oplus M_i) = \oplus J(M_i)$.

    (b) Prove that , if $\{M_i\}$ is a family of $R$-modules, then

$$\oplus J(M_i) \subseteq J(\prod M_i) \subseteq \prod J(M_i).$$

    Give examples to show that both containments may be proper.

53. (a) Show that for an $R$-module $M$, $J(R)M \subseteq J(M)$. Give an example of a ring $R$ and a finitely generated $R$-module $M$ such that $J(R)M \neq J(M)$.

(b) Prove that, if $P$ is a projective $R$-module, then $J(R)P = J(P)$. [Hint: Use Exercise 52 to prove it for free modules, then for projective modules.]

(c) Let $R$ be a left artinian ring, and let $M$ be a left $R$-module. Prove that $J(R)M = J(M)$, and that $M/J(M)$ is the "maximal semisimple factor module" of $M$ (give a precise statement of what that phrase means).

54. Let $P$ be a finitely generated projective left $R$-module and let $S = End_R(P)$. This exercise outlines a proof that $J(S) = \{\alpha \in S : \alpha P \subseteq J(R)P\}$ and $S/J(S) \approx End_R(P/J(R)P)$. Note that this generalizes Exercise 16.

(a) Let $\alpha \in S$ and assume that $\alpha P \subseteq J(R)P$. Show that $(1+\alpha)S = S$. [Hint: Use Nakayama's Lemma to prove that $1 + \alpha$ is surjective.]

(b) Again, let $\alpha \in S$, but assume that there is a maximal proper submodule $P'$ of $P$ with $\alpha P \not\subseteq P'$. Show that there exists $\beta \in S$ with $(1 - \beta\alpha)P \subseteq P'$. [Hint: Note that $\alpha P + P' = P$; hence, given $x \in P, x = \alpha y + z$ for some $y \in P, z \in P'$. Show that we can choose $y = \beta x$ for some $\beta \in S$. To do this, first let $P'' = \{y \in P : \alpha y \in P'\}$ and find $f : P \longrightarrow P/P''$ such that, if $x = \alpha y + z$ as above, then $y + P'' = f(x)$.]

(c) Prove that $J(S) = \{\alpha \in S : \alpha P \subseteq J(R)P\}$, and find an isomorphism

$$S/J(S) \xrightarrow{\approx} End_R(P/J(R)P).$$

# 3

# Central Simple Algebras

In the first two chapters we studied rings and modules. Many of the important examples we studied, such as polynomial rings, matrix rings, group rings and the quaternions, have additional structure we have been ignoring; namely, they are modules as well as rings, and the ring multiplication is compatible with the module multiplication. Thus, these objects are algebras (for definitions and basic properties concerning algebras, see Chapter 0). We now wish to exploit this additional structure in order to learn more about these and other examples.

We will also introduce the tensor product as a way of constructing new algebras from old ones (for definitions and basic properties concerning the tensor product of modules, see Chapter 0). Changing from our philosophy of looking at one ring or module at a time, we view the tensor product as an operation on the category of all algebras over a given field. This point of view (and the tensor product) will be indispensible in our discussion of the Brauer group in Chapter 4. Added motivation for the following material comes from the fact that algebras and the tensor product are useful in algebra, topology, differential geometry and analysis, and indeed occupy a central place in mathematics.

We assume throughout that $k$ is a field, and that, unless otherwise specified, all algebras are $k$-algebras and all tensoring is done over $k$. Sometimes the $k$ may be included for emphasis.

## Tensor Product of Algebras

If $R$ and $S$ are $k$-modules then $R \otimes_k S$ is a $k$-module (see Chapter 0 for details). We now introduce additional structure into the situation in the hope of extracting more information.

If $R$ and $S$ have the additional structure of $k$-algebras, then $R \otimes_k S$ has a $k$-algebra structure such that

$$(r \otimes s) \cdot (r' \otimes s') = rr' \otimes ss' \qquad \text{for all } r, r' \in R \text{ and } s, s' \in S.$$

To justify this, note that $(r, s, r', s') \longmapsto rr' \otimes ss'$ is multilinear, and thus induces a map

$$(R \otimes S) \otimes (R \otimes S) \longrightarrow R \otimes S.$$

Equivalently, there is a bilinear map

$$(R \otimes S) \times (R \otimes S) \longrightarrow R \otimes S.$$

This says that there is a multiplication on $R \otimes S$ which distributes over addition. It is not difficult to see that $1 \otimes 1$ is the identity element for this multiplication, since multiplication by $1 \otimes 1$ fixes all generators $r \otimes s$ of $R \otimes S$. A similar argument (checking on generators) proves that multiplication is associative. Thus we have shown that $R \otimes S$ is a ring. It is also easy to check, using the fact that the ring multiplication in both $R$ and $S$ is compatible with the action of $k$ on these as $k$-modules, that the ring multiplication is compatible with the action of $k$ on the module $R \otimes S$. This shows that $R \otimes S$ is, in fact, a $k$-algebra.

We now look at some of the basic properties of $R \otimes S$. Recall that there are two basic $k$-algebra maps

$$i : R \longrightarrow R \otimes S \qquad \text{and} \qquad j : S \longrightarrow R \otimes S$$

given by

$$r \longmapsto r \otimes 1 \qquad \text{and} \qquad s \longmapsto 1 \otimes s$$

If $\{e_\alpha\}$ is a basis for $S$ over $k$, then every element $x \in R \otimes S$ has a unique expression

$$x = \sum r_\alpha \otimes e_\alpha = \sum (r_\alpha \otimes 1)(1 \otimes e_\alpha) = \sum i(r_\alpha) j(e_\alpha).$$

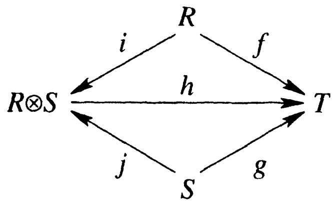
In other words, if we regard $R \otimes S$ as an $R$-module via $i$, then $R \otimes S$ is free with basis $\{j(e_\alpha)\}$. This can be verified by using universal mapping properties to exhibit the coordinate functions. It follows that $i$ is one-to-one, since anything in the kernel would annihilate $R \otimes S$, but only 0 annihilates a free module. Reversing the roles of $S$ and $R$ gives similar results. Since $i$ and $j$ are both one-to-one, we will henceforth identify $R$ and $S$ with their images under $i$ and $j$ (note that the images commute since $(r \otimes 1)(1 \otimes s) = (r \otimes s) = (1 \otimes s)(r \otimes 1)$). With these identifications, our observations above may be stated as follows:

**Proposition 3.1** *Given a field $k$ and $k$-algebras $R$ and $S$, then $R \otimes S$ is a $k$-algebra. Further, we have that:*

*(i) $R \otimes S$ contains $R$ and $S$ as commuting subalgebras.*
*(ii) Any basis $\{s_\beta\}$ of $S$ over $k$ is a basis for $R \otimes S$ as an $R$-module.*
*(iii) Any basis $\{r_\alpha\}$ of $R$ over $k$ is a basis for $R \otimes S$ as an $S$-module.*

Analogous to the universal mapping property of $R \otimes S$ as a module, $R \otimes S$ also has a universal mapping property as an algebra:

**Proposition 3.2** *Given any k-algebra T, and any pair of k-algebra homomorphisms* $R \xrightarrow{f} T, S \xrightarrow{g} T$ *such that* $f(R)$ *and* $g(S)$ *commute and* $f|_k = g|_k$*, then there is a unique k-algebra homomorphism* $h : R \otimes S \longrightarrow T$ *such that* $hi = f$ *and* $hj = g$ *(where i and j denote the canonical inclusions). That is, the following diagram commutes :*




**Proof:** This is similar to the proof of the universal mapping property of the tensor product of modules given in Chapter 0, so we leave this proof as an exercise for the reader. □

The above proposition shows that we can think of $R \otimes S$ as the $k$-algebra generated by $R$ and $S$, subject to the relation that $R$ and $S$ commute. Note that this does not say that $r \otimes s = s \otimes r$ for $r \in R, s \in S$, but that $(r \otimes 1)(1 \otimes s) = (1 \otimes s)(r \otimes 1)$. The universal mapping property of $R \otimes S$ as a $k$-algebra is often used to construct $k$-algebra maps from $R \otimes S$ to $T$, given $k$-algebra maps from $R$ to $T$ and from $S$ to $T$. Examples of this are scattered throughout the text.

## Extension of Scalars and Semisimplicity

We now apply the above comments to an important special case. Suppose we are given a $k$-algebra $R$ and an extension field $K$ of $k$. The elements of $k$ are called **scalars** in the algebra $R$. It would be useful if we could "extend" the scalars of $R$ so that $R$ could be considered as an algebra over $K$. As we shall see, this can be accomplished by using the tensor product, namely by taking $K \otimes_k R$.

First note that any field extension $K$ of $k$ can be considered as an algebra over $k$ since $K$ is a vector space over $k$, elements of $K$ can be multiplied together, and this multiplication is consistent with the scalar multiplication for $K$ as a vector space over $k$. Thus $K \otimes_k R$ is a $K$-algebra, usually written as $R_K$, and is said to be obtained from $R$ by **extension of scalars**. More concretely, this means the following : a $k$-algebra $R$ is often described by giving a basis $\{e_i\}$ of $R$ over $k$ and saying how to multiply basis elements; say

$$e_i e_j = \sum_k c_{ijk} e_k \ , \ c_{ijk} \in k.$$

According to part (ii) of Proposition 3.1, $R_K$ can be described as a $K$-algebra with the same basis and same multiplication law as $R$ over $k$; for note that $k \subseteq K$, so $c_{ijk} \in K$, and the following diagram is commutative :

$$\begin{array}{ccc} k & \longrightarrow & R \\ \downarrow & & \downarrow \\ K & \longrightarrow & K \otimes_k R \end{array}$$

**Example:** Given any real algebra $S$ (i.e., $S$ is an algebra over $\mathbf{R}$), we can construct the $\mathbf{C}$-algebra $S_{\mathbf{C}}$ , which is called the **complexification** of $S$. Note that, taking $S = \mathbf{R}$, then $S_{\mathbf{C}}$ is simply $\mathbf{C}$. $\mathbf{H}_{\mathbf{C}} = \mathbf{C} \otimes_{\mathbf{R}} \mathbf{H}$ is a 4-dimensional $\mathbf{C}$-algebra. We shall later see that this $\mathbf{C}$-algebra is simple, and in fact isomorphic to $\mathcal{M}_2(\mathbf{C})$.

**Remark:** For those who know some category theory, let $\mathbf{R} - \mathbf{Mod}$ denote the category of $R$-modules and $R$-module homomorphisms and let $\mathbf{k} - \mathbf{Alg}$ denote the category of $k$-algebras and $k$-algebra homomorphisms. Then extension of scalars gives a functor from $\mathbf{R} - \mathbf{Mod}$ to $\mathbf{R_K} - \mathbf{Mod}$ and from $\mathbf{k} - \mathbf{Alg}$ to $\mathbf{K} - \mathbf{Alg}$. This may help when thinking about the following comment.

Classically, enlarging the real numbers to the complex numbers often simplified both proofs and statements of theorems; for $\mathbf{C}$ has many useful properties which $\mathbf{R}$ does not, such as being algebraically closed. Extension of scalars is a generalization of this philosophy, and is an important tool that we will make significant use of.

An algebra is said to be a **simple algebra** or a **semisimple algebra** if it has the corresponding property as a ring. We now wish to study the effect that extending scalars has on the semisimplicity of an algebra. We begin with a useful lemma : the Primitive Element Theorem. We include this basic theorem from field theory for those who happened not to have seen it.

**Lemma 3.3 (Primitive Element Theorem)** *If $K \supseteq k$ is a finite separable field extension, then there exists $c \in K$ with $K = k(c)$.*

**Proof:** If $k$ is finite then the proof is easy, so suppose $k$ is infinite. By using induction (which applies since the extension is finite), it suffices to show that $K = k(a,b)$ implies $K = k(c)$ for some $c \in K$. Let $f(x)$ be the irreducible polynomial of $a$ over $k$ with roots $a_1(= a), \ldots, a_n$, and let $g(x)$ be the irreducible polynomial of $b$ over $k$ with roots $b_1(= b), \ldots, b_m$. Since $k$ is infinite, there is some $\alpha \in k$ such that the elements $a_i + \alpha b_j$ are all distinct. Let $c = a + \alpha b$. Now $g(b) = 0$ and $b$ is also a root of $f(c - \alpha x)$ since $f(c - \alpha b) = f(a) = 0$, ;hence $x - b$ divides both $g(x)$ and $f(c - \alpha x)$ in $k(c)[x]$. Since the roots of $f(x)$ and $g(x)$ are distinct (remember $K/k$ is separable), we have that the g.c.d. of $g(x)$ and $f(c - \alpha x)$ in $k(c)[x]$ is $x - b$. Hence $b \in k(c)$. Since $\alpha \in k(c)$ as well, $a = c - \alpha b \in k(c)$. This shows that $k(a,b) \subseteq k(c)$ and so completes the proof. □

The element $c$ in the above lemma is called a **primitive element** for the extension $K \supseteq k$.

Given a finite field extension $L$ of $k$, $L$ is semisimple (as an algebra over $k$) since $L$ is a field. It is natural to ask, more generally: "When is $L_K$ semisimple for every extension of scalars $K \supseteq k$?". For finite extensions, it turns out that $L_K$ is semisimple for all $K$ precisely when $L$ is separable over $k$. This is the content of the following theorem.

**Theorem 3.4** *Let $L/k$ be a finite field extension. Then $L_K = K \otimes_k L$ is semisimple for every field $K \supseteq k$ if and only if $L/k$ is a separable extension.*

**Proof:** Assume that $L$ is separable. By the Primitive Element Theorem, $L = k(\theta)$ for some $\theta \in L$, and hence has a basis $1, \theta, \theta^2, \ldots, \theta^{n-1}$, where $\theta$ satisfies a separable irreducible polynomial $f$ over $k$ of degree $n = [L : k]$; i.e., $L \approx k[x]/(f(x))$. By the above remarks, $L_K$ has the same basis $1, \theta, \theta^2, \ldots, \theta^{n-1}$ over $K$ and satisfies the same polynomial $f$, so $L_K \approx K[x]/(f(x))$. Since $f$ is separable, it factors over $K$ into distinct irreducible polynomials $f(x) = f_1(x) \cdots f_n(x)$ in $K[x]$. So by the Chinese Remainder Theorem (Exercise 1 of Chapter 0), we see that $L_K \approx \prod K[x]/f_i(x)$, a product of fields, and is thus semisimple.

Conversely, assume that $L$ is not separable. Then there exists a $\theta \in L$ which is not a separable element; that is, the minimal polynomial $f(x)$ of $\theta$ over $L$ is not a separable polynomial. Hence there is a field $K \supseteq L$ in which $f(x)$ has repeated factors, so that $k(\theta)_K \approx K[x]/f(x)$ has nilpotent elements. Since $L_K \supseteq k(\theta)_K$, $L_K$ also has nilpotent elements, hence by Corollary 2.5 is not semisimple. □

**Remark:** For the proof it was useful to think of $K \otimes_k L$ as $L_K$, an extension of scalars of $L$. Sometimes, however, it is useful to restate the result in a more symmetric fashion, namely:

*The tensor product of two field extensions of $k$ is semisimple provided one of the factors is finite and separable over $k$.*

## Tensor Products, Simplicity and Semisimplicity

In the last section we studied when extension of scalars gives a semisimple algebra. Now we consider the behavior of semisimplicity and other properties of algebras under tensor products in general.

We define the **center** of an algebra $S$ over $k$ to be $Z(S) = \{x \in S | xs = sx$ for all $s \in S\}$; that is, $Z(S)$ is just the center of $S$ considered as a ring. Note that for an algebra $S$ over $k$, it is always true that $k \subseteq Z(S)$. If, in fact, $k = Z(S)$, we say that $S$ is a **central** $k$-algebra . We call $S$ **central simple** if $S$ is both central and simple.

**Examples:**

1. **H** is a central simple algebra over **R**.
2. Any matrix algebra over a field is central simple (by Exercises 5 and 13(b) of Chapter 1).
3. Any proper field extension $K \supsetneq k$ is not central since $Z(K) = K \supsetneq k$.

We now explore how these properties behave under the operation of tensor product, and determine the structure of the center and the two-sided ideals of a tensor product of certain algebras. Apart from general interest and usefulness, added motivation for this exploration comes from material we will study in Chapter Four. In that chapter we will define a certain group (the Brauer group) whose elements are equivalence classes of certain central simple algebras, with $\otimes$ as the product operation. Corollary 3.6 shows that the group is closed under this product operation.

**Theorem 3.5** *Let $S$ be a central simple algebra and let $R$ be an arbitrary algebra. Then*

1. *Every two-sided ideal of $R \otimes S$ has the form $I \otimes S$, where $I$ is a two-sided ideal of $R$. In particular, if $R$ is simple then $R \otimes S$ is simple.*
2. *$Z(R \otimes S) = Z(R)$. Taking $R = K$, $K$ a field, shows that $S_K$ is a central simple $K$-algebra.*

We shall see from the proof of the theorem that for a given ideal $J$ of $R \otimes S$, the ideal $I$ is unique, and in fact $I = J \cap R$. Before proving the theorem we give one immediate corollary:

**Corollary 3.6** *If $R$ and $S$ are central simple algebras, then so is $R \otimes S$.*

This corollary shows that $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{H}$ is central simple,and that $\mathcal{M}_n(k) \otimes S$ is central simple for any central simple algebra $S$. The converse to Corollary 3.6 is also true (see Exercise 5).

The following lemma will aid us in proving Theorem 2:

**Lemma 3.7** *Let $R$ and $S$ be algebras with $S$ central simple. If $J$ is a non-zero two-sided ideal of $R \otimes S$, then $J \cap R \neq 0$.*

**Proof:** Choose $x \in J, x \neq 0$ so that $x$ is written as a linear combination $x = \sum_{i=1}^{l} r_i \otimes s_i$ with $l$ minimal. Note that $\{r_i\}$ is linearly independent over $k$, for otherwise $l$ would not be minimal; similarly for $\{s_i\}$. Now $s_1 \neq 0$, so by simplicity of $S$ we have $Ss_1S = S$. Thus there exist $x_j, y_j \in S$ with $\sum_{j=1}^{m} x_j s_1 y_j = 1$. Consider

$$\begin{aligned} x' &= \textstyle\sum_{j=1}^{m} (1 \otimes x_j) x (1 \otimes y_j) \\ &= \textstyle\sum_{j=1}^{m} \sum_{i=1}^{l} r_i \otimes x_j s_i y_j \\ &= \textstyle\sum_{i=1}^{l} r_i \otimes (\sum_{j=1}^{m} x_j s_i y_j) \\ &= \textstyle\sum_{i=1}^{l} r_i \otimes s_i' \end{aligned}$$

where $s_i' = \sum_{j=1}^{m} x_j s_i y_j$, so $s_1' = 1$. Clearly $x' \in J, x' \neq 0$ since the $r_i$ are linearly independent over $k$ and hence over $S$ by Proposition 3.1, and $s_1' = 1 \neq 0$. Now for any $s \in S$ we have

$$\begin{aligned} (1 \otimes s)x' - x'(1 \otimes s) &= \textstyle\sum_{i=1}^{l} r_i \otimes ss_i' - \sum_{i=1}^{l} r_i \otimes s_i's \\ &= \textstyle\sum_{i=2}^{l} r_i \otimes (ss_i' - s_i's) \end{aligned}$$

since $ss_1' - s_1's = s - s = 0$. By minimality, this element is zero. Since the $r_i$ are linearly independent over $k$, $ss_i' - s_i's = 0$ for each $i$. But this holds for all $s \in S$, so $s_i'$ is in the center of $S$ for each $i$. Since the center of $S$ is just $k$ by hypothesis (so $r_i \otimes s_i' = r_i \otimes (s_i' \cdot 1) = r_i s_i' \otimes 1$), we have

$$\begin{aligned} x' &= \textstyle\sum r_i \otimes s_i' \\ &= \textstyle\sum r_i s_i' \otimes 1 \\ &= (\textstyle\sum r_i s_i') \otimes 1 \in R. \end{aligned}$$

Since $x' \neq 0$, $x' \in J \cap R \neq 0$ and we are done. □

With this lemma at our disposal we now prove Theorem 2:

**Proof:** We begin with a proof of part (i) of the theorem. Let $J$ be a two-sided ideal of $R \otimes S$ and let $I = J \cap R$. Consider the natural map $R \otimes S \longrightarrow (R/I) \otimes S$. We claim that the kernel of this map is $I \otimes S$ : for if $\{x_i\}$ is a basis for $I$, extend this to a basis $\{x_i\} \cup \{y_j\}$ for $R$; then $\{y_j + I\}$ is a basis for $R/I$. Hence $\sum a_i x_i + \sum b_j y_j$ is in the kernel if and only if $b_j = 0$ for all $j$. Considering

$$J \longrightarrow (R \otimes S)/(I \otimes S) \approx (R/I) \otimes S,$$

in order for $J$ to contain $I \otimes S$ properly it must be that the image of this map is non-zero, so by the lemma $im(J) \cap R/I \neq 0$. But $im(J) \cap R/I = 0$ by the choice of $I = J \cap R$. This proves part (i) of the theorem.

Our proof of part (ii) does not depend on the fact that $S$ is simple: Let $z = \sum r_i \otimes s_i$ be in the center of $R \otimes S$. As in the proof of Lemma 3.7, we may assume that the $r_i$ are linearly independent over $k$. For $s \in S$ we have

$$0 = (1 \otimes s)z - z(1 \otimes s) = \sum r_i \otimes (ss_i - s_i s).$$

The independence of the $r_i$ over $S$ then gives $ss_i - s_i s = 0$ for all $i$, so $ss_i = s_i s$; that is, $s_i \in Z(S) = k$ for all $i$. Thus

$$\begin{aligned} z &= \sum r_i \otimes s_i \\ &= \sum r_i s_i \otimes 1 \\ &= (\sum r_i s_i) \otimes 1 \\ &= r \otimes 1 \end{aligned}$$

where $r = \sum r_i s_i$. If $x \in R$, then

$$0 = (x \otimes 1)z - z(x \otimes 1) = (xr - rx) \otimes 1,$$

so $xr = rx$ for all $x \in R$; i.e., $r \in Z(R)$. □

We now have the necessary tools to answer questions concerning semisimplicity of tensor products of certain semisimple algebras. But first two

**Remarks:**

**1.** For algebras $R = R_1 \times R_2$, we have $R \otimes S \approx (R_1 \otimes S) \times (R_2 \otimes S)$ for any algebra $S$. To see this, note that the map

$$R \times S \longrightarrow (R_1 \otimes S) \times (R_2 \otimes S)$$

$$(r_1, r_2, s) \longmapsto (r_1 \otimes s, r_2 \otimes s)$$

is bilinear with respect to $R$ and $S$, and thus induces a homomorphism $R \otimes S \longrightarrow (R_1 \otimes S) \times (R_2 \otimes S)$. It is then easy to check that this is an isomorphism by writing down the obvious inverse (using the injections $R_i \hookrightarrow R, i = 1, 2$). By induction, $(\prod R_i) \otimes S \approx \prod(R_i \otimes S)$ for any finite product of rings.

**2.** Suppose $S$ is a simple $k$-algebra with center $C$. Chapter 1, Exercise 13 shows that $C$ is a field, so we can view $S$ as a central simple $C$-algebra. It is not hard to show (Exercise 13) that $C \approx End_{S\otimes S^\circ}(S)$. It is also clear that $R \otimes_k S = (R \otimes_k C) \otimes_C S$.

We may use these remarks to reduce questions concerning semisimplicity of tensor products of semisimple algebras to easier questions. Remark (1) reduces the question to the case of simple algebras. Remark (2) further breaks down the question into two steps : first do the extension of scalars case, then answer the question assuming one of the algebras is central. We shall use this method when proving Proposition 3.9.

In order to talk about semisimplicity of extension of scalars, we needed the notion of separable field extension. Discussing semisimplicity of tensor products requires a generalization of this concept.

**Definition:** Suppose $S$ is a finite dimensional semisimple algebra over $k$. If $C$ denotes the center of $S$, then $C = C_1 \times \cdots \times C_k$ where the $C_i$ are fields (see Chapter 1, Exercise 13). We say that $S$ is a **separable algebra** if every $C_i$ is separable over $k$. Equivalently, we say that $S$ is separable if for each simple $S$-module $M$, the center of $End_S(M)$ is a separable field extension of $k$.

The notion of separable algebra vastly generalizes that of separable field extension. We saw in the previous section that for such extensions $L$, all extensions of scalars $L_K$ are semisimple. We now prove the analogous result for the more general case of separable algebras.

**Proposition 3.8** *If $S$ is a separable algebra, then $S_K$ is semisimple for all fields $K \supseteq k$.*

**Proof:** We may assume by Remark (1) that $S$ is simple with separable center $C$. Remember that $C$ is a field since $S$ is simple. Now

$$
\begin{aligned}
K \otimes S &\approx (K \otimes C) \otimes_C S && \text{by Remark (2)} \\
&\approx (\textstyle\prod R_i) \otimes_C S && \text{for some simple } R_i \text{ by Theorem 3.4} \\
&\approx \textstyle\prod (R_i \otimes_C S) && \text{by Remark (1)}
\end{aligned}
$$

and each $R_i \otimes_C S$ is simple by part (i) of Theorem 2, since each $R_i$ is simple and $S$ is central simple over $C$. □

Continuing the generalization of results on separable field extensions to separable algebras, we now prove a fact analogous to the statement that the tensor product of two field extensions is semisimple provided one of the factors is finite and separable.

**Proposition 3.9** *If $R$ and $S$ are finite dimensional semisimple algebras, and if at least one of $R$ and $S$ is separable, then $R \otimes S$ is semisimple.*

**Proof:** Without loss of generality suppose $R$ is separable. By Remark (1), we may assume that both $R$ and $S$ are simple. Let $C$ denote the center of $S$; so $C$ is a field. Then

$$
\begin{aligned}
R \otimes S &\approx (R \otimes C) \otimes_C S && \text{by Remark (2)} \\
&\approx (\textstyle\prod R_i) \otimes_C S && \text{for some simple } R_i \text{ by the previous proposition} \\
&\approx \textstyle\prod (R_i \otimes_C S) && \text{by Remark (1)}
\end{aligned}
$$

and each $R_i \otimes_C S$ is simple for the same reasons as in the previous proposition. □

# Some Applications of Tensor Products

The results of the previous section have many interesting consequences. To begin with, we obtain some nice results on the dimension of certain finite dimensional algebras. Knowing the dimension of an algebra vastly limits the possibilities of what that algebra can be. This will be useful when we are trying to determine what the alternatives are for finite dimensional division algebras over various fields (e.g., the reals). The following proof provides us with our first example of how information may be obtained by extending scalars to a field where more is known. This technique is extremely useful for a variety of problems.

**Theorem 3.10** *If $D$ is a finite dimensional division algebra over its center $k$, then $[D : k]$ is a square.*

**Proof:** Let $K = \overline{k}$, the algebraic closure of $k$. Note that $[D : k] = [D_K : K]$. $D_K$ is a finite dimensional algebra over $K$, hence artinian. Also, $D_K$ is simple by part (i) of Theorem 2. Thus, by the Structure Theorem for Simple Artinian Rings, $D_K$ is isomorphic to a ring of $n \times n$ matrices with coefficients in a (finite dimensional) division algebra over $K$. Since $K$ is algebraically closed, Exercise 1 of Chapter 0 tells us that the only finite

dimensional division algebra over $K$ is $K$ itself; hence $D_K \approx \mathcal{M}_n(K)$. So $[D : k] = [D_K : K] = [\mathcal{M}_n(K) : K] = n^2$. □

More generally, if $A$ is a simple algebra which is finite dimensional over its center $Z$, then, by the Structure Theorem for Simple Artinian Rings, $A \approx \mathcal{M}_n(D)$, where $D$ is a finite dimensional (over $Z$) division algebra with center $Z$. So

$$\begin{aligned}[A : Z] &= [A : D][D : Z] \\ &= n^2 \cdot [D : Z] \\ &= n^2 \cdot m^2 \qquad \text{for some } m, \text{ by Theorem 3.10} \\ &= (nm)^2.\end{aligned}$$

This proves

**Corollary 3.11** *If $A$ is a simple algebra which is finite dimensional over its center $Z$, then $[A : Z]$ is a square.*

It is no surprise that a matrix algebra has dimension which is a square, for we can plainly "see" the $n^2$ dimensions. The fact that *any* simple algebra of finite dimension actually has square dimension is quite remarkable, however, for it is far from obvious given the definitions. How useful it is to extend scalars!

We prove the next result with an eye towards Chapter 4. As already mentioned, we shall construct a group (the Brauer group of a field $k$) whose elements are certain equivalence classes of finite dimensional central simple algebras over $k$, with $\otimes$ acting as product in the group. It will turn out that $\mathcal{M}_n(k)$ will be in the equivalence class of the identity. The following proposition uses Theorem 2 to show that the inverse (in the Brauer Group) of the equivalence class of a central simple algebra $R$ is the equivalence class of $R^\circ$. This comment will be made precise in Chapter 4.

**Proposition 3.12** *Let $R$ be a finite dimensional central simple algebra. Then $R \otimes R^\circ \approx \mathcal{M}_n(k)$, where $n = [R : k]$.*

**Proof:** Let

$$A = \{L_r \in End_k(R) : L_r(x) = rx, r \in R\}$$

$$B = \{T_r \in End_k(R) : T_r(x) = xr, r \in R\}.$$

Then, as shown in Chapter 1, $A \approx R$ and $B \approx R^\circ$ as rings. Also, elements of $A$ and $B$ commute by the associativity law in $R$ (yes, the *associativity* law). Define

$$R \otimes R^{\circ} \longrightarrow End_k(R)$$

by

$$r \otimes s \longmapsto L_r \circ T_s.$$

Since $R$ (and thus $R^{\circ}$) is central simple, by Theorem 2 we have that $R \otimes R^{\circ}$ is simple. Thus the map is one-to-one. Since $dim_k(R \otimes R^{\circ}) = (dim_k(R))^2 = dim_k(End_k(R))$, we know that the map is onto, and thus an isomorphism. Since $\mathcal{M}_n(k) \approx End_k(R)$ we are done. □

**Remark:** This is the second proof of this result. The earlier proof (Corollary 1.17), used simplicity to show the above map is onto, then computing dimension showed that the map is one-to-one.

Exercise 25 of Chapter 1 shows that $\mathbf{H} \approx \mathbf{H}^{\circ}$. Since $\mathbf{H}$ is a central simple algebra of dimension 4 over $\mathbf{R}$, the theorem tells us that $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{H} \approx \mathcal{M}_4(\mathbf{R})$. This provides yet another proof that $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{H}$ is central simple.

# The Skolem-Noether Theorem

It is easy to show (Exercise 15), using elementary linear algebra, that any automorphism of the ring of $n \times n$ matrices over a field $k$ which leaves $k$ fixed must be inner (i.e., the automorphism is "conjugation by a fixed matrix"). The Skolem-Noether Theorem is an important generalization of this fact to any finite dimensional central simple algebra. In order to prove this theorem, we need to know that for finite dimensional simple algebras $R$, there is a unique $R$-module (up to isomorphism, of course) of any given dimension. This is the content of

**Lemma 3.13** *Let $R$ be a finite dimensional simple algebra over $k$. If $M_1$ and $M_2$ are finite dimensional $R$-modules of the same dimension over $k$, then $M_1 \approx M_2$.*

**Proof:** Since $R$ is finite dimensional (hence artinian) and simple, we know by the Structure Theorem for Simple Artinian Rings that $R$ has a unique simple module $M$. Then $M_1 \approx M^{l_1}$ and $M_2 \approx M^{l_2}$ for some $l_1, l_2$. Clearly $dim_k(M_i) = l_i dim_k(M)$ for $i = 1, 2$, so if $dim_k(M_1) = dim_k(M_2)$, then $l_1 = l_2$ and hence $M_1 \approx M_2$. □

The above lemma generalizes the well-known fact that any two vector spaces (over a field) of the same dimension are isomorphic. With this lemma in hand we are now ready to prove the Skolem-Noether Theorem.

**Theorem 3.14 (Skolem-Noether)** *Let $S$ be a finite dimensional central simple $k$-algebra, and let $R$ be a simple $k$-algebra. If $f, g : R \longrightarrow S$ are homomorphisms (necessarily one-to-one), then there is an inner automorphism $\alpha : S \longrightarrow S$ such that $\alpha f = g$.*

*Equivalently, If $R_1$ and $R_2$ are isomorphic simple subalgebras of $S$, then for any homomorphism $f : R_1 \longrightarrow R_2$ there is an inner automorphism $\alpha$ of $S$ such that $\alpha|_{R_1} = f$. In particular, any automorphism of $S$ is inner.*

**Note:** We cannot drop the assumption that the center of $S$ is $k$. For example, if $S$ is a proper field extension of $k$, then there are usually many $k$-algebra automorphisms of $S$, but there are no (non-trivial) inner ones since $S$ is commutative. As a special case, note that complex conjugation is a non-inner $\mathbf{R}$-algebra automorphism of $\mathbf{C}$.

**Proof:** $S$ is finite dimensional (hence artinian) and simple, so $S \approx End_D(V)$ for some division algebra $D$ over $k$ and some finite dimensional $D$-module $V$. Note that $Z(S) = Z(D) = k$. Now $f$ and $g$ define two $R$-module structures on $V$ which commute with the given action of $D$ and which induce the given $k$-module structure on $V$. Hence $V$ is an $R \otimes D$-module in two different ways. But $R \otimes D$ is artinian and simple (by Theorem 2), so by the Lemma these two $R \otimes D$-modules are isomorphic; that is, there is an abelian group isomorphism $h : V \longrightarrow V$ such that

$$\begin{aligned} &(1) \quad h(f(r)v) = g(r)h(v) \quad \text{and} \\ &(2) \quad h(dv) = dh(v) \end{aligned}$$

Now (2) says that $h \in End_D(V) = S$, and (1) says that $hf(r) = g(r)h$; that is, $hf(r)h^{-1} = g(r)$. This finishes the proof. □

The Skolem-Noether Theorem will play a crucial role in our proofs of two classical theorems of Wedderburn and Frobenius, as well as in the construction of factor sets, which will be objects of study in Chapter 4. In case this is not enough to emphasize the usefulness of the Skolem-Noether Theorem, several more of its many applications are given in the exercises at the end of this chapter.

## The Centralizer Theorem

In the study of groups it is quite useful to study the centralizers of various subgroups of a group. In this section, we define the centralizer in the context of algebras, and prove an important result on centralizers which will help to elucidate the structure of algebras.

**Definition:** If $R$ is an algebra and $S$ is any subset of $R$, the **centralizer of $S$ in $R$** is defined to be $C(S) = \{r \in R | rs = sr \text{ for all } s \in S\}$. One may check that $C(S)$ is a subalgebra of $R$ for any subset $S \subseteq R$.

For a central simple $k$-algebra $S$, $C(C(S)) = C(k) = S$ by definition. In other words, $S$ is its own "double centralizer" . Intuitively, it seems as if the smaller the subalgebra $R$, the larger the centralizer $C(R)$ should be, for it is easier to commute with fewer elements. Taking the double centralizer $C(C(R))$ is like moving "up and down", then. Of course it is always true that $R \subseteq C(C(R))$. Part (iv) of the following theorem shows that, as in the case of the centralizer of the full central simple algebra, moving up and down actually takes one back to where one started.

If $S$ is a finite dimensional simple algebra, then by the Structure Theorem for Simple Artinian Rings we know that $S \approx \mathcal{M}_n(D)$ for some $n$ and some division algebra $D$. In fact, it makes sense to talk about *the* division ring $D$ such that $S \approx \mathcal{M}_n(D)$, for $D$ is uniquely determined (up to isomorphism) as the opposite of the endomorphism ring of the unique simple $S$-module. We shall write $S \sim D$ when $S \approx \mathcal{M}_n(D)$ for some $n$. The relation $\sim$ is a special case of a more general relation which will be of importance in Chapter 4, where we will discuss the set of central simple algebras under that equivalence relation. We shall elaborate fully on these ideas in Chapter Four.

**Theorem 3.15 (Centralizer Theorem)** *Let $S$ be a finite dimensional central simple algebra over $k$, and let $R$ be a simple subalgebra of $S$. Then*

*(1) $C(R)$ is simple.*
*(2) If $S \sim D_1$ and $R \otimes D_1^\circ \sim D_2$, then $C(R) \sim D_2^\circ$.*
*(3) $[S : k] = [R : k][C(R) : k]$.*
*(4) $C(C(R)) = R$.*

**Remarks:**

**1.** Note that Parts 2 and 3 completely determine the structure of $C(R)$.

**2.** Part 4 of this theorem is often called the "Double Centralizer Theorem".

**Proof:** By the Structure Theorem for Simple Artinian Rings, we may assume that $S \approx End_D(V) \approx \mathcal{M}_n(D^\circ)$, where $D$ is a division algebra with center $k$ and $V$ is a finite dimensional $D$-module. Also note that $V$ is an $R \otimes D$-module, and $C(R) = End_{R\otimes D}(V) \subseteq S$.

Proof of Part 1: $R \otimes D$ is simple, so $R \otimes D \approx End_E(W)$, where $W$ is the unique simple $R \otimes D$-module and $E = End_{R\otimes D}(W)$ is the associated division algebra. So $V \approx W^m$ as $R \otimes D$-modules. Thus

$$\begin{aligned} C(R) &\approx End_{R\otimes D}(W^m) \\ &\approx \mathcal{M}_m(End_{R\otimes D}(W)) \quad \text{by Prop. 1.7} \\ &\approx \mathcal{M}_m(E). \end{aligned}$$

Proof of Part 2: $S \sim D^\circ$, so $D_1 = D^\circ$. Now $R \otimes D_1^\circ = R \otimes D \sim E^\circ = D_2$ (by the above). Thus $C(R) \sim E = D_2^\circ$.

Proof of Part 3: Since $C(R) \approx \mathcal{M}_n(E)$, we have that $[C(R) : k] = n^2[E : k]$. Since $V \approx W^n$ we also have that $[V : k] = n[W : k] = n[W : E][E : k]$. Squaring this and plugging back in to the first equality gives

$$\begin{aligned}
[C(R) : k] &= \frac{[V : k]^2}{[W : E]^2[E : k]^2}[E : k] \\
&= \frac{[V : k]^2}{[W : E]^2[E : k]} \\
&= \frac{[V : k]^2}{dim_k(End_E(W))} \\
&= \frac{[V : k]^2}{[R : k][D : k]}
\end{aligned}$$

and so

$$\begin{aligned}
[R : k][C(R) : k] &= \frac{[V : k]^2}{[D : k]} \\
&= \frac{[V : D]^2[D : k]^2}{[D : k]} \\
&= [S : k].
\end{aligned}$$

Proof of 4: Applying Part 3 to $C(R)$ gives $[S : k] = [C(R) : k][C(C(R)) : k]$, so $[C(C(R)) : k] = [R : k]$. Also note that $R \subseteq C(C(R))$, so clearly $R = C(C(R))$. □

Among the Centralizer Theorem's many applications, we can now express any finite dimensional central simple algebra in terms of any of its central simple subalgebras:

**Corollary 3.16** *If $R$ is a central simple subalgebra of a finite dimensional central simple algebra $S$, then $S \approx R \otimes C(R)$.*

**Proof:** Since $R$ and $C(R)$ commute, we have a map $R \otimes C(R) \longrightarrow S$ via $r \otimes r' \mapsto rr'$. Since $R \otimes C(R)$ is simple, this map is one-to-one, hence an isomorphism by counting dimensions. □

With a little more work it is possible to make the technique of extension of scalars even more useful. The idea is to try to extend scalars "as little

as possible", but enough so that things become easy. We shall now make this precise.

Let $D$ be a division algebra over $k$. A field $K \supseteq k$ such that $D_K \approx \mathcal{M}_n(K)$ is called a **splitting field** for $D$; for in this case $D_K$ splits as a sum of $n$ simple $K$-modules, whereas $D$ is simple as a module over itself. A central simple $k$-algebra of the form $\mathcal{M}_n(k)$ is often called a **split** central simple $k$-algebra. If $K$ is a separable maximal subfield of the $k$-algebra $D$, and if $L$ is an extension of $k$ which splits every polynomial $f(x) \in k[x]$ having a root in $K$, then $L$ splits $D$ (see Chapter 4, Exercise 30). This gives a connection between the word "splitting" used in two different ways.

The integer $n$ is called the **degree** of $D$; $n^2$ is called the **rank** of $D$ over $k$. Note that no further splitting takes place when we extend scalars over $K$; for if $K' \supseteq K$, then

$$\begin{aligned} D_{K'} &\approx K' \otimes_K D_K \\ &\approx K' \otimes_K \mathcal{M}_n(K) \\ &\approx \mathcal{M}_n(K'). \end{aligned}$$

In the next chapter we will use this technique to split the collection of all division algebras with center $k$ into more manageable pieces. These pieces will turn out to have another explicit description via homological algebra.

As another application of the Centralizer Theorem, we derive a useful result on maximal subfields of a division algebra $D$ and their relationship to the existence of splitting fields for $D$.

**Corollary 3.17** *Let $D$ be a division algebra with center $k$ and $[D : k] = n^2$. If $K$ is any maximal subfield of $D$, then $[K : k] = n$. Moreover, $K$ is a splitting field for $D$.*

**Proof:** The first part follows immediately from parts (3) and (4) of the Centralizer Theorem; for $C(K) = K$, so $n^2 = [D : k] = [K : k][C(K) : k]$.

To show that $K$ is a splitting field for $D$, we note that $D$ is a $D$-$K$ bimodule (for the definition of bimodule, see Exercise 28 of Chapter 0), hence a $D \otimes K$-module, and as such it is simple. Moreover, $End_{D\otimes K}(D) = K$. Since $D \otimes K$ is simple, it follows that $D \otimes K \approx End_K(D) \approx M_m(K)$, $m = [D : K]$. □

Corollary 3.17 provides us with many examples of splitting fields. It is also true that for any division algebra there always exists a maximal subfield which is also separable (see Exercise 33). This will be important in our study of the Brauer group in Chapter 4.

# Some Famous Theorems

The material presented so far in this chapter is mostly useful as a tool for further applications. The power of these results may not seem obvious at first, so at this point we will attempt to convert the unconvinced. A good way to do this, perhaps, is to use the results to prove two famous, classical theorems.

**Theorem 3.18 (Wedderburn's Theorem)** *Every finite division ring is commutative.*

This theorem (an addition to our growing list of "Wedderburn Theorem"s!) is truly remarkable in that commutativity properties of a ring seem to have nothing at all to do with whether or not the ring is finite; although the theorem proves our intuition completely wrong. Apart from being surprising and beautiful in its own right, this result (originally proven by Wedderburn in 1905) has played an important role in many areas of algebra, such as representation theory and projective geometry (see, e.g. E. Artin, *Geometric Algebra*). This theorem is also a foundation stone for an extensive theory dealing with conditions that can be put on a ring that will make it commutative. For further details, see Herstein, *Noncommutative Rings.*

The following proof, due to B. L. van der Waerden , uses the Skolem-Noether Theorem and consequences of the Centralizer Theorem in an essential way.

**Proof:** For a finite division ring $D$, let $k = Z(D)$ (remember that the center of a division ring is a field), and let $K$ be a maximal subfield of $D$ containing $k$, so $k \subseteq K \subseteq D$. If $K = D$ we are done, so assume $K \neq D$. By Theorem 3.10 we have $[D : k] = n^2$ for some $n$, so (since $K \neq D$) we have $[K : k] = n$ by Corollary 3.17. Thus if $q = |k|$, then $K$ must have order $q^n$.

Now any two fields containing $k$ of order $q^n$ are isomorphic, since they are both splitting fields of the polynomial $x^{q^n} - x$ over $k$ (see, e.g., Jacobson, *Basic Algebra I*, Chapter 4.13). Thus they are conjugate in $D$ by the Skolem-Noether Theorem. Every element of $D$ is contained in some maximal subfield of $D$, so $D = \bigcup_{x \in D} xKx^{-1}$ for some fixed maximal subfield $K$. If $D^*$ denotes the multiplicative group of $D$, then $D^* = \bigcup_{x \in D^*} xK^*x^{-1}$. But this is impossible unless $K = D$ since, as shall be proved in the following lemma, no finite group is a union of conjugates of any nontrivial subgroup. □

We now prove the lemma that was necessary in the above proof. This lemma is an elementary problem in group theory.

**Lemma 3.19** *If $H < G$ are finite groups with $H \neq G$, then $G \neq \bigcup_{g \in G} gHg^{-1}$.*

**Proof:** If $N(H)$ denotes the normalizer of $H$ in $G$, then $[G : N(H)]$ is the number of subgroups in $G$ which are conjugate to $H$. The number of non-identity elements in $\bigcup_{g\in G} gHg^{-1}$ is

$$\begin{aligned} &\leq [G : N(H)](|H| - 1) \\ &\leq [G : H](|H| - 1) \\ &= |G| - [G : H] \\ &< |G| - 1 \qquad\qquad \text{since } H \neq G \end{aligned}$$

and so $G \neq \bigcup_{g\in G} gHg^{-1}$. □

In Chapter 4 we will give another (less elementary) proof of Wedderburn's Theorem by showing that the Brauer group of a finite field is trivial.

We know that $\mathbf{C}$ and $\mathbf{H}$ are division algebras of dimensions 2 and 4, respectively, over $\mathbf{R}$. What are the other finite dimensional division algebras over $\mathbf{R}$? W.R. Hamilton, who discovered the quaternions in 1843, had worked for ten years trying to come up with a division algebra of dimension 3 over $\mathbf{R}$. Of course Theorem 3.10 tells us that such an algebra does not exist, and so (fortunately) Hamilton did not succeed. After Hamilton tried in dimension 4 and succeeded in constructing the quaternions, efforts were made by many mathematicians to come up with other so-called "hypercomplex systems" (i.e., finite dimensional division algebras over $\mathbf{R}$). All of these efforts failed. Thus it was indeed satisfying when, in 1878, Frobenius showed that all such hypercomplex systems had already been found :

**Theorem 3.20 (Frobenius)** *If $D$ is a division algebra with $\mathbf{R}$ in its center and $[D : \mathbf{R}] < \infty$, then $D = \mathbf{R}, \mathbf{C}$, or $\mathbf{H}$.*

**Proof:** Let $K$ be a maximal subfield of $D$, so $[K : \mathbf{R}] < \infty$ by the given. Since the only finite field extensions of $\mathbf{R}$ are $\mathbf{R}$ and $\mathbf{C}$(Chapter 0, Exercise 34), we have that $[K : \mathbf{R}] = 1$ or 2. If $[K : \mathbf{R}] = 1$, then by Corollary 3.17 we have that $[D : \mathbf{R}] = 1$ and so $D = \mathbf{R}$. If $[K : \mathbf{R}] \doteq 2$, then again by Corollary 3.17 we have $[D : K] = 1$ or 2. If $[D : K] = 1$ then $D = \mathbf{C}$, so suppose that $[D : K] = 2$. Now $K \approx \mathbf{C}$, and the map $f : K \longrightarrow K$ given by $a + bi \longmapsto a - bi$ is an $\mathbf{R}$-isomorphism. Hence, by the Skolem-Noether Theorem, there exists $x \in D$ with $x(a+bi)x^{-1} = a-bi$ for all $a, b$. It is easy to check that conjugation by $x^2$ is the identity, and so $x^2 \in C(K) = K$. Now $f(x) = x^2$, and so $x^2 \in \mathbf{R}$. If $x^2 > 0$, then $x^2 = r^2$ for some $r \in \mathbf{R}$, so $x = \pm r$, a contradiction. Thus $x^2 < 0$, and so $x^2 = -y^2$ for some $y \in \mathbf{R}$. Let $j = x/y$, and let $k = ij$. It is then easy to check that

$$\begin{aligned} i^2 &= j^2 = k^2 = -1 \\ ij &= k = -ji \\ jk &= i = -kj \\ ki &= j = -ik. \end{aligned}$$

We also leave it for the reader to check (see Exercises 16) that $\{1, i, j, k\}$ form a basis for $D$. □

In particular, this theorem shows that the only finite dimensional central division algebras over **R** are **R** and **H**. In Chapter 4 we will use a calculation of the Brauer group of **R** to recover this result.

In our definition of an algebra, we assumed associativity of multiplication. If this restriction is dropped, then there is a (non-associative) division algebra over **R** of dimension 8 called the Cayley Algebra , otherwise known as the octonions, and denoted by **O**. There is a theorem, the Generalized Frobenius Theorem , that says that **R**, **C**, **H**, and **O** are the only finite dimensional division algebras over **R**. This result is quite satisfying in the sense that it tells us that "we know everything" about finite dimensional division algebras over **R**.

## Summary

In this chapter we explored properties of central simple algebras over a field $k$. We saw that the tensor product $A \otimes_k B$ of any two $k$-algebras $A$ and $B$ is itself a $k$-algebra in the obvious way, and that $A \otimes_k B$ is central simple if both $A$ and $B$ are. This fact was used to show that, for a separable $k$-algebra $S$, the $K$-algebra $S_K$ is semisimple for any extension $K$ of the scalars $k$, generalizing the case when $S$ is a separable field extension of $k$. We also saw that any automorphism of a finite dimensional central simple algebra $S$ is inner (Skolem-Noether Theorem), and that the double centralizer of any simple subalgebra of $R$ of $S$ is $R$ itself (Double Centralizer Theorem). These two Theorems were used to prove the classical results that any finite division ring is commutative (another Wedderburn Theorem), and that the only finite dimensional division algebras containing **R** in its center are **R**, **C**, and the real quaternions **H** (Frobenius Theorem). Thus all such division algebras over **R** were classified. In Chapter 4, we shall use the material developed in this chapter in an attempt to prove theorems along the lines of the Frobenius Theorem, and along the way we will get a glimpse of how this material ties in with a myriad of fields, including number theory and algebraic K-theory.

# Exercises

1. Let $R$ be a $k$-algebra and let $V$ be a vector space over $k$. Regard $V$ as a subspace of $R \otimes V$ in the usual way.

   (a) For any subspace $W$ of $V$, show that $(R \otimes W) \cap V = W$.

   (b) If $W_1$ and $W_2$ are subspaces of $V$ such that $R \otimes W_1 = R \otimes W_2$, show that $W_1 = W_2$. Show that this assertion is not necessarily true unless $k$ is a field. [Hint: try $k = \mathbf{Z}$.]

2. Given finite groups $G = G_1 \times G_2$ and a field $k$, show that

$$k[G] \approx k[G_1][G_2] \approx k[G_1] \otimes k[G_2]$$

   as $k$-algebras.

3. Let $R$ be a finite-dimensional central simple k-algebra. If $M$ is an $R$-$R$-bimodule relative to $k$, show that $M$ is free both as a left $R$-module and as a right $R$-module. In fact, show that there exists a subset of $M$ which is a basis of $M$ both as a right and left $R$-module. In particular, deduce that if $R$ is a subalgebra of an algebra $S$, then $S$ is a free $R$-module. [Hint: $M$ is an $R \otimes_k R^\circ$-module and hence its structure is completely known.]

   **Remark:** The results of this problem, except possibly for the existence of a simultaneous basis, remain valid even if $k$ is not the center of $R$. The proof again uses tensor products, but in a different way. For details, see Bourbaki, *Algebra*, Chapter 8, section 5.

4. Let $\mathbf{H}$ be the division ring of quaternions over $\mathbf{R}$.

   (a) Show that $\mathbf{H}_{\mathbf{C}}$ is isomorphic to $\mathcal{M}_2(\mathbf{C})$.

   (b) Explicitly exhibit this isomorphism, i.e., compute the images of all the basis vectors $1 \otimes 1, 1 \otimes i, 1 \otimes j, 1 \otimes k$ of $\mathbf{H}_{\mathbf{C}}$ over $\mathbf{C}$. [Hint: Find a simple $\mathbf{H}_{\mathbf{C}}$-module.]

5. Let $R$ and $S$ be algebras.

   (a) Show that both $R$ and $S$ are simple (semisimple) if $R \otimes S$ is simple (semisimple).

   (b) Show that both $R$ and $S$ are central if $R \otimes S$ is central.

6. Let $R$ be an artinian algebra and let $S$ be a finite dimensional algebra. Prove that $R \otimes S$ is artinian.

7. (a) Let $R$ be a finite-dimensional commutative algebra over a field $k$. If $R$ is semisimple, show that every subalgebra of $R$ is also semisimple.

   (b) Give an example to show that this is false in the noncommutative case. In fact, give a commutative subalgebra of $\mathcal{M}_2(k)$ which is not semisimple, even though $\mathcal{M}_2(k)$ is simple.

8. (a) If $R$ is a finite-dimensional algebra over a field $k$, and if $R$ is also an integral domain, show that $R$ is a division algebra over $k$.

   (b) Prove that a subalgebra of a finite-dimensional division algebra is also a division algebra.

9. (a) Let $f(x) \in k[x]$, $k$ a field. Show that $k[x]/(f(x))$ is semisimple if and only if $f(x)$ is a separable polynomial over $k$ (i.e., has no multiple roots in its splitting field). [Hint: Use unique factorization and the Chinese Remainder Theorem.]

   (b) Let $K$ be a finite dimensional separable extension field of a field $k$, and let $A$ be a central simple $K$-algebra. Show that $A \otimes_k A^\circ$ is not simple. [Hint: Find an idempotent $\neq 0, 1$ in $K \otimes_k K^\circ$.]

10. Let $S$ be a finite dimensional semisimple algebra over a field $k$. Show that $S$ is a separable $k$-algebra if and only if $S$ is projective as an $S \otimes_k S^\circ$-module.

### Filling in Some Holes

The following exercises come from assorted gaps we have left in the text. You will be doing the authors a great service if you work these problems out.

11. (a) Prove Proposition 3.2

    (b) Deduce from this that if $M$ is an $R$-module and an $S$-module such that the two actions commute and induce the same $k$-module structure on $M$, then there is a unique $R \otimes S$-module structure on $M$ inducing the given actions of $R$ and $S$.

12. Furnish another proof of Theorem 3.4 by showing that $K[x]/(f(x))$ has no nilpotent elements.

13. Let $S$ be a simple algebra with center $C$. Show that $C \approx End_{S \otimes S^\circ}(S)$.

14. Check that the two "equivalent" definitions of separable algebra given on page 89 are really equivalent.

15. Show, using only elementary linear algebra, that any automorphism of the ring of $n \times n$ matrices over a field $k$ which leaves $k$ fixed is inner (i.e., the automorphism is "conjugation by a fixed matrix"). [Hint: Let $V = k^n$ be the vector space. Note that the images of the elementary linear transformations (given by multiplication) $e_{11}, e_{22}, \ldots, e_{nn}$ on this vector space are one-dimensional and have sum equal to $V$. If $f$ is any automorphism of $\mathcal{M}_n(k)$, then $f(e_{11}), \ldots, f(e_{nn})$ have the same property. Use these subspaces to give bases for $V$, and show that the action of $f$ is the same as conjugation by this change of basis matrix. It will be useful to note that a matrix is completely determined by its product with the $e_{ii}$.]

16. Check that the properties of $i, j$, and $k$ given in the proof of Theorem 3.20 hold. Also check that $\{1, i, j, k\}$ is indeed a basis for $D$.

### Altering the Hypotheses of Skolem-Noether (or trying to)

17. Let $k$ be a field, $S = \mathcal{M}_5(k), R = k \times \mathcal{M}_2(k)$. Define $f, g : R \longrightarrow S$ by $f(x,y) = diag(x,y,y)$ and $g(x,y) = diag(x,x,x,y)$, where diag denotes the appropriate block matrix. Show that there is no inner automorphism $h$ of $S$ such that $hf = g$. Hence the Skolem-Noether theorem cannot be generalized to include the case of semi-simple subalgebras of a central simple algebra.

18. In our proof of the Skolem-Noether Theorem we assumed that the ring $S$ had finite dimension over its center $k$. It is only necessary to assume that the embedded simple algebra $R$ has finite dimension over $k$. Check that every step of the given proof works for this case, except possibly the last step: $S = End_D(V)$ for $D$ a division algebra with center $k$, $V$ a finite dimensional vector space over $D$. $V$ is a module over $R \otimes_k D$ in two different ways, via $f, g : R \longrightarrow S$. As before, $V$ is still a finitely generated $R \otimes D$-module and as such is still the sum of a finite number of copies of the unique simple $R \otimes D$-module. We no longer know that the same number occur each time since the dimensions over $k$ could be infinite. Nevertheless, we can still get a map $j : V \longrightarrow V$ from "$V$ with $f$-structure" to "$V$ with $g$-structure" (if the first number of summands is smaller; in the opposite direction if the reverse is true) which satisfies : (i) $j$ is one-to-one; and (ii) $j \circ f(r) = g(r) \circ j$. If $j$ had an inverse, the proof would be complete.

    Complete the following two ideas to show that any element of an artinian ring which is not a zero-divisor must be a unit, thus finishing the above proof in two different ways :

    (i) Use Fitting's Lemma (Chapter 0, Exercise 50).

    (ii) Alternatively, show that it suffices to prove the statement for the ring mod its radical, which has no radical and is artinian; hence is

semisimple. Now use the Wedderburn Structure Theorem to reduce the problem to the case of matrix algebras over a field. Prove the statement in this case by considering row and column reductions.

19. This exercise shows that the Skolem-Noether Theorem does not necessarily hold if the simple subalgebras in question are not finite dimensional.

(a) Let $R_1 \subseteq R_2 \subseteq \cdots$ be a (not necessarily finite) increasing sequence of simple rings. Show that the union $\bigcup_i R_i$ is simple.

(b) Let $S$ be a central simple $k$-algebra which is not commutative; for example, $S$ could be $\mathcal{M}_2(k)$. Let $S_i$ denote the tensor product (over $k$) of $i$ copies of $S$. Let $R = \bigcup_i S_i$. Show that $R$ is a central simple $k$-algebra.

(c) Pick any element $s \in S$ which is not central. Use this to give a conjugation on each $S_i$ which is nontrivial on each factor of the tensor product. Show that this induces an automorphism of $R$ which is not inner.

(d) Consider the following subalgebras of $R$:

$$R_{\text{odd}} = S \otimes_k 1 \otimes_k S \otimes_k 1 \otimes_k \cdots$$
$$R_{\text{even}} = 1 \otimes_k S \otimes_k 1 \otimes_k S \otimes_k \cdots$$

Use these subalgebras to show that the first part of the Skolem-Noether Theorem does not necessarily hold if the subalgebras are not finite dimensional.

20. What happens if we replace the central simple algebra $S$ in the Skolem-Noether Theorem with a semisimple ring? Show that with the appropriate centralizer assumption, the first part of the theorem will still hold, but the second part will not. What happens if one drops the assumption that the ring homomorphisms take 1 to 1?

21. Compute the automorphism group of an arbitrary semisimple ring. [Hint: Reduce the question to that of the homogeneous components and note that endomorphisms can be described in matrix notation. When does such a matrix really represent an automorphism?]

### More on Centralizers

22. Let $A$ and $B$ be $k$-algebras.

(a) Show that the centralizer of $A \otimes k$ in $A \otimes B$ is equal to $Z(A) \otimes B$, where $Z(A)$ denotes the center of $A$.

(b) Show that $Z(A \otimes B) = Z(A) \otimes Z(B)$.

(c) Show that if $C$ and $D$ are subalgebras of $A$ and $B$, respectively, then the centralizer of $C \otimes D$ in $A \otimes B$ is isomorphic to the tensor product of the centralizer of $C$ in $A$ with the centralizer of $D$ in $B$.

23. Let $A$ be a $k$-algebra with subalgebra $B$. Prove that if $x \in A^*$, then $C(x^{-1}Bx) = x^{-1}C(B)x$.

24. Prove the following generalization of the Centralizer Theorem : If $S$ is a central simple $k$-algebra (not necessarily of finite dimension), and if $R$ is a finite dimensional simple subalgebra of $S$, then $C(R)$ is simple, and $C(C(R)) = R$. [Hint: Use the generalized form of the Skolem-Noether Theorem (Exercise 18)and the previous two exercises.]

## Another Theorem of Wedderburn

**Theorem 3.21** *Let $A$ be a finite dimensional algebra over a field $k$. Let $I$ be a two-sided ideal of $A$ which is generated by nilpotent elements. Then $I$ is nilpotent.*

25. Prove this theorem as follows :

(i) We may as well assume that $k$ is algebraically closed since $A$ is a subring of $\overline{k}\otimes_k A$, where $\overline{k}$ denotes the algebraic closure of $k$. Explain.

(ii) Show that $\mathcal{M}_n(k)$ does not have a basis over $k$ consisting of nilpotents. [Hint: consider the trace.]

(iii) We now proceed by using induction on the dimension of I over $k$. Why does the case $dim(I) = 1$ work?

(iv) Now $I$ is artinian and if $I$ contains no nilpotent left ideals, so $I$ is semisimple by Theorem 2.4. Hence $I \approx \prod M_{n_i}(k)$. Why are these matrix rings over $k$?

(v) By (ii) this can't happen. Thus $I$ contains a nonzero nilpotent left ideal. Thus $J(R) \cap I \neq 0$.

(vi) Consider $A/(J(R) \cap I)$ and compute the $k$-dimension of the image of $I$. Use the induction hypothesis to complete the proof.

26. (a) Wedderburn's Theorem (Theorem 3.21, that is!) is usually stated for rings without unit: If $I$ is a finite dimensional $k$-algebra which has a basis consisting of nilpotent elements, then $I$ is nilpotent (here $I$ need not have an identity element). Show that this follows from the Wedderburn theorem by taking $A = k \oplus I$ with suitably defined multiplication. Conversely, the above theorem follows from this one.

(b) Apply this theorem to give another proof of Problem 49 in Chapter 2, which states that, for a finite $p$-group $G$ and a field $k$ of characteristic $p > 0$, the augmentation ideal $I$ is the Jacobson radical of $k[G]$ and hence $k[G]$ is a local ring.

**Remarks:**

**(i)** Actually, the augmentation ideal $I$ is generated by elements of the form $s - 1$, where $s$ runs over a set of group elements which generate $G$. Prove this as an exercise.

**(ii)** This material plays a crucial role in the Nakayama-Rim theory of cohomologically trivial modules. For more information on this topic, see K. Brown, *Cohomology of Groups.*

## Applications of the Skolem-Noether Theorem

27. Let $D$ be a finite dimensional division algebra over its center $k$. Let $a, b \in D$ have the same minimal polynomial over $k$. Show that there exists $x \in D$ such that $xbx^{-1} = a$. This result is due to Dickson.

28. (a) Let $U$ denote the elements of absolute value 1 in $\mathbf{H}$, the real quaternions. Prove that every element in $U$ is a commutator in the multiplicative group $\mathbf{H}^*$ of $\mathbf{H}$. In fact, show that one can take the elements to lie in $U$ itself. Further, prove that given any triple of elements $u_1, u_2, u_3$ in $U$, there exists elements $z, v_1, v_2, v_3$ in $U$ with $u_1 = [z, v_1], u_2 = [z, v_2], u_3 = [z, v_3]$. Can this be done with an arbitrary 4 elements of $U$? [Hint: Use the previous exercise, and note that two elements of $U$ have the same minimal polynomial if and only if they have the same trace.]

    (b) Let $D$ be a division algebra of dimension 4 over its center. Prove that every pair of commutators in $D^*$ can be written as commutators with the same first (or last) element. Use this to conclude that every element of $[D^*, D^*]$ can be represented as a single commutator.

29. Let $D$ be a division algebra containing a finite field $k$ in its center. Assume that every element of $D$ satisfies an algebraic equation over $k$. Prove that $D$ is a field. [Hint: Let $K$ be the center of $D$ and take $x \in D, x \notin K$. Show that there is an element $y \in D$ such that $yk[x]y^{-1} = k[x]$ but $yxy^{-1} \neq x$. Obtain a contradiction by looking at $k[x, y]$.]

30. Let $R$ be a ring. An additive map $d : R \longrightarrow R$ is called a **derivation** if $d(ab) = ad(b) + d(a)b$. For example, differentiation of polynomials is a derivation on the ring of polynomials over $\mathbf{R}$. $d$ is called an **inner derivation** if there exists an element $c \in R$ such that $d(x) = xc - cx$ for all $x \in R$.

    **Theorem 3.22** *Let $R$ be a finite dimensional central simple $k$-algebra. Every $k$-linear derivation on $R$ is inner.*

Prove this theorem by applying the Skolem-Noether Theorem to the following two isomorphic subrings of $\mathcal{M}_2(R)$:

$$\{rI : r \in R\} \qquad \text{and} \qquad \left\{ \begin{bmatrix} r & d(r) \\ 0 & r \end{bmatrix} : r \in R \right\}$$

**Remark:** Derivations play an important role in the study of separable algebras, a concept vastly generalizing separable field extensions. The degree to which derivations fail to be inner can be measured by a certain cohomology group, which we shall discuss later.

31. Let $k$ be a field of characteristic not equal to 2. Let $D$ be a division algebra over $k$ such that $[D : k] = 4$. Suppose that $D$ is not commutative. Show that $k$ is the center of $D$ and that there exists elements $u, v \in D$ so that $1, u, v, uv$ form a basis for $D$ over $k$ and satisfy $u^2 = a, v^2 = b, uv = -vu$ for some $a, b \in k$. Such an algebra is called a **generalized quaternion algebra** over $k$. These algebras play an important role in the study of the Brauer group and in algebraic K-theory, and are discussed in greater detail in the exercises of Chapter 4.

### The Jacobson-Noether Theorem

**Theorem 3.23 (Jacobson-Noether)** *If $D$ is a noncommutative division ring which is algebraic over its center $k$, then there is an element in $D$, not in $k$, which is separable over $k$.*

32. Prove this theorem as follows:

(a) Let $K \supseteq k$ be fields of characteristic $p$ and let $c \in K$ be algebraic over $k$. Let $f(x)$ be the minimal polynomial of $c$ over $k$. If $f(x)$ has multiple roots, show that $f(x) = g(x^p)$ for some $g(x) \in k[x]$. Conclude that $f(x) = h(x^{p^e})$ for some $h(x) \in k[x]$ which has no multiple roots. This says that $c^{p^e}$ is separable over $k$.

(b) Since the theorem is clear if $k$ has characteristic 0, assume that $k$ has characteristic $p > 0$. If the theorem fails, show (using part (a)) that there exists $a \in D$ with $a^p \in k, a \notin k$. Define $d : D \longrightarrow D$ by $d(x) = xa - ax$. Show that $d$ is a $k$-linear map which satisfies $d \neq 0$ and $d^p(x) = xa^p - a^p x$. Hence $d^p = 0$ since $a^p \in k$. Let $y \in D$ be such that $d(y) \neq 0$ and choose $s$ such that $x = d^{s-1}(y) \neq 0$ and $d^s(y) = 0$. Now $s > 1$ so $x = d(w)$ for some $w \in D$, i.e., $x = wa - aw$. Further, $dx = 0$, i.e. $ax = xa$. Write $x = au$. Show that $a = ca - ac$ for $c = wu^{-1}$. Thus $c = 1 + aca^{-1}$. Raise this to a large power of $p$ and reach a contradiction.

33. (a) (Koethe's Theorem) Use the Jacobson-Noether Theorem to show that if $D$ is a finite dimensional division algebra with center $k$, and if $K \subseteq D$ is a separable extension of $k$, then $D$ has a maximal subfield containing $K$ which is separable over $k$.

(b) Conclude from the Jacobson-Noether Theorem that any central simple algebra has a separable splitting field which is finite dimensional over its center.

(c) Does there exist a maximal subfield which is galois (i.e., normal and separable) over its center? [Remark: Don't feel bad if you don't get this one, considering that this was an open question for quite some time. The problem was finally answered in the negative by Amitsur (See S. Amitsur, "On Central Division Algebras", or B. Jacob and A. Wadsworth, "A new construction of noncrossed product algebras").]

### Embeddings of Algebras

34. (a) Let $D$ be a central division $k$-algebra, $A = \mathcal{M}_r(D)$, and $V$ be a simple $A$-module. Describe $[V : k]$ in terms of $r$ and $D$.

(b) Let $A$ be a central simple $k$-algebra with $[A : k] = n^2$. Given a matrix algebra $\mathcal{M}_m(k)$, it is natural to ask under what conditions on $A$ does $A$ embed as a subalgebra of $\mathcal{M}_m(k)$. There is a nice answer to this question. First note that $A \approx \mathcal{M}_m(D)$ for a unique division algebra $D$ by the Structure Theorem for Simple Artinian Rings, and $[D : k] = d^2$ for some integer $d$ by Theorem 3.10 (we will later call $d$ the "Schur index" of $A$ in studying the Brauer group). Prove that $A$ is isomorphic to a $k$-subalgebra of $\mathcal{M}_m(k)$ if and only if $nd$ divides $m$. In particular, show that if $A$ is a central division $k$-algebra then this condition holds if and only if $[A : k]$ divides $m$. [Hint: Use the Centralizer Theorem and Wedderburn's Theorem.]

35. (a) More generally, suppose that $A_1$ and $A_2$ are simple $k$-algebras with $A_2$ central. Let $D_i$ $(i = 1, 2)$ be the unique division algebra with $A_i \approx \mathcal{M}_{r_i}(D_i)$; and let $n_i = [A_i : k]$, $d_i = [D_i : k]$ $(i = 1, 2)$. Note that $n_i = r_i d_i$. Note that $A_1 \otimes D_2^\circ$ is simple, so $A_1 \otimes D_2^\circ \approx \mathcal{M}_{r_3}(D_3)$ for a unique division algebra $D_3$; let $d_3 = [D_3 : k]$. Prove that $A_1$ embeds as a $k$-subalgebra of $A_2$ if and only if $n_1 d_2 d_3$ divides $n_2$. [Hint: Let $V_i$ $(i = 1, 2)$ be the simple $A_i$ module, and let $V_3$ be the simple $A_1 \otimes D_2^\circ$-module. First show that $A_1$ embeds in $A_2$ if and only if $V_2$ is isomorphic to some $A_1 \otimes D_2^\circ$-module. Show that this holds if and only if $dim_k(V_3)$ divides $dim_k(V_2)$. Now compute dimensions of everything in sight.]

(b) What happens if $A_1$ is now just semisimple in the above? How about if $A_2$ is semisimple? How about if both $A_1$ and $A_2$ are just semisimple? What kind of theorem can you prove?

## The Cartan-Brauer-Hua Theorem

36. This problem provides two lemmas which will be used in the proof of the Cartan-Brauer-Hua Theorem (Exercise 37).

    (a) Let $R$ be a finite dimensional algebra over an infinite field $k$. Show that if $r \in R$, then there exists $s \in k^*$ with $r - s$ a unit in $R$. In particular, show that every element of $R$ is the sum of two units in $R$. [Hint: Since $R$ is finite dimensional, $f(r) = 0$ for some non-zero polynomial $f \in k[x]$. Since $k$ is infinite, there exists $s \in k^*$ such that the polynomial $f(x + s)$ has a non-zero constant term.]

    (b) Show that no group can be written as the union of two of its proper subgroups.

37. Prove the Cartan-Brauer-Hua Theorem: Let $R$ be a finite dimensional central simple algebra over an infinite field $k$. If $D$ is a division subalgebra of $R$ with $D^*$ a normal subgroup of $R^*$, then either $D = k$ or $D = R$. [Hint: Suppose $D \neq k$ and $D \neq R$. Use part (a) of Exercise 36 to show that $D^*$ is properly contained in $R^*$, and use the Double Centralizer Theorem to show that $C(D)$ is properly contained in $R$. Now apply part (b) of Exercise 36 to find an element $x \in (D^* \cup C(D)^*)$ with $x \notin R^*$. Use the hypothesis and part (a) of Exercise 36 to show that $w \in D^*$, giving a contradiction.]

38. (a) Show that every subalgebra of a division algebra is a division algebra.

    (b) Show that if $D$ is a finite dimensional central division algebra with subfield $E \neq k$, then $D$ is generated (as a $k$-algebra) by $\bigcup_{d \in D^*} d^{-1}Ed$.

    (c) Use part (b) of this exercise to give another proof of Wedderburn's Theorem that finite division rings are commutative. Notice that this gives a proof of Wedderburn's theorem via the Double Centralizer Theorem, whereas the proof given in the text uses the Skolem-Noether Theorem.

# 4

# The Brauer Group

This chapter is concerned with the classification of finite dimensional central division algebras over a given field $k$. In the case $k = \mathbf{R}$, the Frobenius Theorem shows that $\mathbf{R}$ and $\mathbf{H}$ are the only finite dimensional central division algebras over $\mathbf{R}$. This kind of classification is optimal in the sense that we have an explicit, easy-to-understand list of all finite dimensional central division algebras over $\mathbf{R}$. Classifying finite dimensional central division algebras over other fields has proven much more difficult, and in fact this problem has been a focal point for research in number theory and quadratic forms. Although such an explicit list as in the case of central division algebras over $\mathbf{R}$ cannot always be given, there is much that can be said.

Our attack on the above problem shall lead us to a discussion of the Brauer group, named for R. Brauer, who first defined this group in 1929. Computing the Brauer group is a classical problem that has strong ties with number theory and algebraic geometry (see, e.g., J.P. Serre , *Local Fields*). The Brauer group has also begun to play an important role in algebraic K-theory, as can be seen by recent work of Merkur'ev and Suslin (see I. Kersten, *Brauergruppen von Körpern*).

We shall assume throughout this chapter that, unless otherwise specified, all of the algebras are finite dimensional.

## An Equivalence Relation on Central Simple Algebras

For reasons that will soon be clear, it is more convenient to rephrase the above classification question as follows: given a field $k$, try to classify all finite dimensional central simple algebras over $k$ up to similarity, where $S$ and $S'$ are called **similar** (written $S \sim S'$) if the division algebras $D, D'$ such that $S \approx \mathcal{M}_n(D)$ and $S' \approx \mathcal{M}_{n'}(D')$ are isomorphic. Note that such division algebras exist by the Structure Theorem for Simple Artinian Rings, and that it makes sense to talk about *the* division algebra such that $S \approx \mathcal{M}_n(D)$ since $D$ is uniquely determined (up to isomorphism) as the opposite of the endomorphism ring of a simple $S$-module. Thus we see that each similarity class contains a unique isomorphism class of finite dimensional

central division algebras, and each such division algebra is contained in a unique similarity class. So the classification problem for finite dimensional central division algebras is equivalent to that for finite dimensional central simple algebras (up to similarity).

The point of studying the set of central simple algebras over $k$ instead of the central division algebras is that the tensor product of two division algebras is not always a division algebra, while the tensor product of two central simple algebras is again a central simple algebra; that is, the set of central simple algebras is closed under tensor product. This allows one to put a group structure on the (similarity classes of) central simple $k$-algebras. The group structure imposes constraints which can be exploited to give information about the central simple $k$-algebras, hence about the central division $k$-algebras.

It will be useful in later discussions to phrase the above equivalence relation in several different, though equivalent, forms.

**Definition:** Let $S$ and $T$ be finite-dimensional central simple $k$-algebras. We say that $S$ and $T$ are **similar** , and write , $\boldsymbol{S \sim T}$ , if any one of the following equivalent conditions hold :

1. If $S \approx \mathcal{M}_n(D)$ and $T \approx \mathcal{M}_m(E)$ for division rings $D, E$, then $D \approx E$.
2. There exist $m, n$ such that $S \otimes_k \mathcal{M}_m(k) \approx T \otimes_k \mathcal{M}_n(k)$.
3. There exist $m, n$ such that $\mathcal{M}_m(S) \approx \mathcal{M}_n(T)$.
4. If $M$ is the unique simple $S$-module and $N$ is the unique simple $T$-module, then $End_S(M) \approx End_T(N)$.

It is not difficult, using the previous discussion and Lemma 4.1, to check that these four definitions of similarity are equivalent. We leave the verification as an exercise to the reader.

## The Brauer Group : Definition and Examples

Finally, after lots of foreshadowing in the previous chapter, we come to the definition of the Brauer group.

**Definition:** The **Brauer group** of a field $k$, denoted $\boldsymbol{Br(k)}$, is the set of equivalence classes of finite-dimensional central simple $k$-algebras under the equivalence relation of similarity, with the tensor product acting as the group operation and the equivalence class of $k$ acting as the identity element. The equivalence class in the Brauer group of a finite-dimensional central simple algebra $S$ will be denoted by $[S]$.

**Note:** For the logicians and set theorists in the crowd, it is an easy exercise to check that the set of isomorphism classes of finite-dimensional algebras over a given field really does form a set.

The Brauer group acts as a "classifier" of central division algebras, in the sense that each element of $Br(k)$ corresponds to a distinct central division algebra over $k$. For example, $Br(k) = 0$ precisely when $k$ is the only central division $k$-algebra. Although we will not always be able to give a list of elements of $Br(k)$ (and thus an explicit classification of central division algebras), the group structure of $Br(k)$ will allow us to make other quantitative statements about the set of such algebras.

Note that $[\mathcal{M}_n(k)] = [k] = 1 \in Br(k)$ for every $n$. It is also useful to note that if $A$ and $B$ are finite-dimensional central simple $k$-algebras, then $A \approx B$ if and only if $[A] = [B]$ in $Br(k)$ and $A$ and $B$ have the same dimension over $k$.

Our next goal is to show that the Brauer group is, in fact, a group. Before doing this, however, we shall give two useful lemmas.

**Lemma 4.1** *(i)* $\mathcal{M}_n(R) \approx R \otimes_k \mathcal{M}_n(k)$ *for any $k$-algebra $R$.*
*(ii)* $\mathcal{M}_m(k) \otimes \mathcal{M}_n(k) \approx \mathcal{M}_{mn}(k)$.

**Proof:** Denoting the $n \times n$ identity matrix in $\mathcal{M}_n(R)$ by $I$, we have maps $R \longrightarrow \mathcal{M}_n(R)$ via $r \mapsto rI$ as well as the natural inclusion $\mathcal{M}_n(k) \longrightarrow \mathcal{M}_n(R)$. Now $(rI)A = rA = Ar = A(rI)$; that is, the images of the above maps commute, and so there is a ring map $R \otimes_k \mathcal{M}_n(k) \longrightarrow \mathcal{M}_n(R)$ with $1 \otimes e_{ij} \mapsto e_{ij}$, where $e_{ij}$ is the elementary matrix with a 1 in the $i, j$ position. Clearly the map takes an $R$-basis to an $R$-basis and is thus an isomorphism.

To prove part (ii), simply let $R = \mathcal{M}_n(k)$ in the above to obtain

$$\begin{aligned} \mathcal{M}_m(k) \otimes \mathcal{M}_n(k) &\approx \mathcal{M}_n(\mathcal{M}_m(k)) \quad \text{by part (i)} \\ &\approx \mathcal{M}_{nm}(k) \end{aligned}$$

The last isomorphism is the "erase-the-lines" isomorphism which comes from facts about block multiplication of matrices. For a slightly more hands-on proof of part (ii), see Exercise 2. □

The next lemma will help show that multiplication in the Brauer group is well-defined by proving that we may multiply two equivalence classes by multiplying any two representatives from these classes and then taking the equivalence class of the product.

**Lemma 4.2** *If $S \sim S_1$ and $T \sim T_1$ then $S \otimes T \sim S_1 \otimes T_1$.*

**Proof:** First note that if $A \sim B$, then $A$ and $B$ have the same division algebra $D$, so we may write

$$\begin{array}{ll} S \approx \mathcal{M}_n(D) & T \approx \mathcal{M}_m(E) \\ S_1 \approx \mathcal{M}_{n_1}(D) & T_1 \approx \mathcal{M}_{m_1}(E) \end{array}$$

for some positive integers $m, n, m_1, n_1$. Then

$$\begin{aligned} S \otimes T &\approx \mathcal{M}_n(D) \otimes \mathcal{M}_m(E) \\ &\approx D \otimes \mathcal{M}_n(k) \otimes E \otimes \mathcal{M}_m(k) && \text{by (i) of Lemma 4.1} \\ &\approx D \otimes E \otimes \mathcal{M}_{nm}(k) && \text{by (ii) of Lemma 4.1 and commutativity of tensor product} \\ &\approx \mathcal{M}_{nm}(D \otimes E) && \text{by (i) of Lemma 4.1} \end{aligned}$$

Similarly, $S_1 \otimes T_1 \approx \mathcal{M}_{n_1 m_1}(D \otimes E)$ and we are done. □

Having given these two lemmas, we need only collect facts from the previous chapter to show that $Br(k)$ is an abelian group.

**Proposition 4.3** *$Br(k)$ with the operation $[S] \bullet [T] = [S \otimes T]$ is an abelian group.*

**Proof:** Let $S$ and $T$ be two finite-dimensional central simple $k$-algebras. Then $S \otimes T$ is finite-dimensional, and by Corollary 3.6 we know that $S \otimes T$ is central simple. From this fact and Lemma 4.2 we see that the tensor product gives a well-defined multiplication on $Br(k)$. Associativity of this multiplication follows from associativity of the tensor product. Clearly $[k]$ acts as an identity element, and by the definition of $\sim$ we have $[\mathcal{M}_n(k)] = [k]$. By Proposition 3.12, $S \otimes S^\circ \approx \mathcal{M}_n(k)$ for a finite-dimensional central simple algebra $S$, which proves that $[S^\circ]$ is the inverse of $[S]$ in $Br(k)$. Finally, $Br(k)$ is abelian since $S \otimes T \approx T \otimes S$ for any algebras $S$ and $T$. □

There are a few cases in which $Br(k)$ can be explicitly computed. Although not all the proofs are contained in this book, we provide the following list of examples to give the reader some idea of the possibilities that are involved.

**Examples:**

1. $Br(F) = 0$ for any finite field $F$ by Wedderburn's Theorem on finite division rings. In fact, $Br(k) = 0$ for any algebraic extension $k$ of a finite field.

2. $Br(k) = 0$ for any algebraically closed field $k$, since there are no (nontrivial) division algebras over an algebraically closed field (Chapter 1, Exercise 1). In fact, $Br(k) = 0$ for any field $k$ of transcendence degree one over an algebraically closed field.

3. $Br(\mathbf{R}) \approx \mathbf{Z}_2$ and is generated by $[\mathbf{H}]$, as shown by Frobenius' Theorem and the fact that $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{H} \approx \mathcal{M}_4(\mathbf{R})$.

4. $Br(\hat{\mathbf{Q}}_p) \approx \mathbf{Q}/\mathbf{Z}$. Here $\hat{\mathbf{Q}}_p$ denotes the field of $p$-adic numbers. The subgroup of $\mathbf{Q}/\mathbf{Z}$ of order $n$ (namely $\frac{1}{n}\mathbf{Z}/\mathbf{Z}$) corresponds to those division algebras which have a splitting field of degree $n$. The proof of this result uses local class field theory and is beyond the scope of this book. The interested reader may consult Serre, *Local Fields*, or Kersten, *Brauergruppen von Körpern.*

5. For the Brauer group of $\mathbf{Q}$, there is an exact sequence

$$0 \longrightarrow Br(\mathbf{Q}) \xrightarrow{j} \bigoplus_i Br(\mathbf{Q}_i) \xrightarrow{f} \mathbf{Q}/\mathbf{Z} \longrightarrow 0$$

   where $\mathbf{Q}_i$ ranges over all completions of $\mathbf{Q}$, $j$ is the canonical map (which maps into the direct sum rather than the direct product since the map $Br(\mathbf{Q}) \longrightarrow Br(\mathbf{Q}_i)$ is trivial for all but finitely many $i$), $f(\{x_i\}) = \sum x_i$, $Br(\mathbf{R})$ is identified with $\frac{1}{2}\mathbf{Z}/\mathbf{Z}$, and each $Br(\mathbf{Q}_p)$ is identified with $\mathbf{Q}/\mathbf{Z}$. One may interpret this result by noting that each element of $Br(\mathbf{Q})$ gives rise to an infinite number of numerical invariants in $\mathbf{Q}/\mathbf{Z}$, which completely determines the element. These invariants can be arbitrary, subject only to : (i) the first is in $\frac{1}{2}\mathbf{Z}/\mathbf{Z}$, (ii) all but a finite number are zero, and (iii) their sum is zero. This can be generalized to other number fields; see Kersten, *Brauergruppen von Körpern.*

In the 1930's, such eminent mathematicians as A.A. Albert, R. Brauer, H. Hasse and E. Noether made an intensive study of $Br(k)$ in the case when $k$ is an algebraic number field. This work, which uses techniques from and has importance in number theory, culminated in the complete determination of the Brauer group of an algebraic number field. One of their results is that any central division algebra over an algebraic number field $k$ is isomorphic to a cyclic crossed product algebra, which we will define later in this chapter. For a summary of this work, see Albert, *Structure of Algebras*, Deuring, *Algebren*, or Pierce, *Associative Algebras.*

## The Relative Brauer Group and Galois Splitting Fields

This section will explore the relationship between the Brauer Group and maximal subfields of central simple algebras. We begin by noting that $Br(\ )$, which associates to each field an abelian group, has the following functorial property : given a field extension $K/k$, there is a homomorphism

$$Br(k) \longrightarrow Br(K)$$

given by

$$[S] \longmapsto [S_K]$$

where $S_K = K \otimes_k S$ is an extension of scalars. This homomorphism can often be used to determine information about $Br(k)$ from information about $Br(K)$, which may be easier to deal with. The above homomorphism also leads us to the following

**Definition:** $Br(K/k) = ker(Br(k) \longrightarrow Br(K))$; that is, $Br(K/k)$ is the set of finite-dimensional central division algebras over $k$ which are split by $K$. $Br(K/k)$ is called the **relative Brauer group** .

The relative Brauer group will be useful in studying the Brauer group, for we will be able to reduce questions about $Br(k)$ to questions about $Br(K/k)$ for certain $K$, and $Br(K/k)$ is often easier to work with. In order to do this we must first discuss a generalization of maximal subfield of a division ring.

**Definition:** Let $S$ be a simple $k$-algebra. A **maximal subfield** of $S$ is defined to be a field $K \subseteq S$ containing $k$ such that $C(K) = K$; that is, $K$ is its own centralizer in $S$.

There is another natural notion of "maximal subfield" meaning a subfield which is maximal with respect to inclusion. The two definitions agree for division algebras, but do not agree in general. In fact, maximal subfields (in the first sense defined above) do not always exist. These facts are illustrated by the following

**Examples:**

1. Consider $\mathcal{M}_n(\mathbf{H})$, which is a simple $\mathbf{R}$-algebra of dimension $4n^2$. By the Centralizer Theorem, any maximal subfield of $\mathcal{M}_n(\mathbf{H})$ would have dimension $2n$ over $\mathbf{R}$. But the only finite extensions of $\mathbf{R}$ are $\mathbf{R}$ and $\mathbf{C}$, so if $n > 1$ then a maximal subfield of $\mathcal{M}_n(\mathbf{H})$ cannot exist.

2. Even when maximal subfields under both definitions exist, the two notions do not always coincide. We give an easier example of when maximal subfields (with our definition) are too small to be maximal commutative subrings. Consider the ring $\mathcal{M}_{2n}(F)$ over a field $F$ and the subring $S \subset \mathcal{M}_{2n}(F)$ of matrices of the form

$$\begin{bmatrix} aI & B \\ 0 & aI \end{bmatrix}$$

where $a \in F$, $I$ is the $n \times n$ identity matrix and $B$ is any $n \times n$ matrix. Then $S$ is a commutative subring of dimension $n^2 + 1$ over $F$, so any maximal commutative subring has dimension at least $n^2 + 1$. By the Centralizer Theorem, however, any maximal subfield of $\mathcal{M}_{2n}(F)$ has dimension $2n$.

Computation of $Br(k)$ is based on a more detailed study of splitting fields than we've given so far. Corollary 3.17 provides us with one example of how to construct splitting fields; namely, as maximal subfields of a division algebra. More generally we have the following

**Theorem 4.4** *Let $S$ be a central simple $k$-algebra of dimension $n^2$. Then any maximal subfield $K$ of $S$ is a splitting field for $S$, and $[K : k] = [S : K] = n$. Conversely, given any field extension $K \supset k$ of degree $n$, any element of $Br(K/k)$ has a unique representative $S$ of degree $n^2$ which contains $K$ as a maximal subfield.*

**Proof:** First note that

$$\begin{aligned} n^2 &= [S:k] && \text{by hypothesis} \\ &= [K:k][C(K):k] && \text{by part (iii) of the Centralizer Theorem} \\ &= [K:k]^2 && \text{since } C(K) = K \end{aligned}$$

and so $[K : k] = n$. To show that $K$ is a splitting field for $S$, note that $S$ acts on $S$ on the left, $K$ acts on $S$ on the right, and the actions commute, thus giving a map

$$f : S \otimes_k K \longrightarrow End_K(S) \approx \mathcal{M}_n(K)$$

where $f(s \otimes x)(s') = ss'x$. Since $S$ is central simple and $K$ is simple, $S \otimes K$ is simple by part (i) of Theorem 2. Since $f$ has simple domain and is clearly nonzero, $f$ is one-to-one. Also, both $S \otimes_k K$ and $\mathcal{M}_n(K)$ have dimension $n^3$ over $k$; hence $f$ is an isomorphism.

Conversely, suppose we are given an extension $K/k$ and an element of $Br(K/k)$. Let $D$ be the division algebra which represents the chosen element of $Br(K/k)$. Then $K \otimes_k D^\circ \approx \mathcal{M}_m(K)$ for some $m(D$ acts on the right) and is thus simple. Also note that

$$[D^\circ : k] = m^2 \qquad (*).$$

Let $V$ be the simple $K \otimes_k D^\circ$-module, so $K \otimes D^\circ \approx V^m$. Computing the dimensions of both sides gives

$$m \cdot [V : D] = [K : k] \qquad (**).$$

Now $K$ acts on $V$, and the action commutes with that of $D$, so there is a $K$-algebra homomorphism

$$K \longrightarrow End_{D^\circ}(V) \approx \mathcal{M}_{[V:D]}(D)$$

which is injective since $K$ is a field. Let $S = \mathcal{M}_{[V:D]}(D)$. Then $[S] = [D]$ in $Br(K/k)$ and

$$\begin{aligned}[S : k] &= [V : D]^2[D : k] \\ &= [V : D]^2 m^2 \quad \text{by } (*) \\ &= ([V : D] \cdot m)^2 \\ &= [K : k]^2 \quad \text{by } (**).\end{aligned}$$

Now an application of part (iii) of the Centralizer Theorem, applied to the simple subalgebra $K$ of the central simple algebra $S$, yields

$$[K : k]^2 = [S : k] = [K : k][C(K) : k]$$

and so $C(K) = K$ and we are done. Uniqueness follows from the dimension of $S$. □

For a division algebra of dimension $n^2$ over its center $k$, there exists a splitting field which is a finite galois extension of $k$. This is trivial to prove when the characteristic of $k$ is zero, or, more generally, when every finite extension of $k$ is separable. The case of an arbitrary field requires use of the Jacobson-Noether Theorem (Chapter 3, Exercise 32), and is done in the following corollary. The fact that a galois splitting field exists is essential when giving an explicit description of elements of the Brauer group.

**Corollary 4.5** *If $D$ is a division algebra with center $k$ and of dimension $n^2$, then there exists a finite galois extension $K$ of $k$ which is a splitting field for $D$.*

**Proof:** It follows from the Jacobson-Noether Theorem that there exists a maximal subfield $L \subset D$ which is separable over $k$ (see Chapter 3, Exercise 33(a)). Let $k \subset L \subset K$ be the normal closure. So $K$ is galois over $k$ and

$$\begin{aligned}D \otimes_k K &\approx (D \otimes_k L) \otimes_L K \\ &\approx \mathcal{M}_n(L) \otimes_L K \\ &\approx \mathcal{M}_n(K)\end{aligned}$$

□

We now draw an immediate but important conclusion from Corollary 4.5. The following corollary reduces the general computation of $Br(k)$ of a field $k$ to the study of $Br(K/k)$ in the case where $K$ is galois over $k$. This is important because the relative Brauer group is, as we shall see in the sections which follow, much easier to compute than $Br(k)$.

**Corollary 4.6** $Br(k) = \bigcup Br(K/k)$, *where $K$ ranges over the finite galois extensions of $k$.*

Corollary 3.17 shows that if $D$ is a division algebra of dimension $n^2$, then any maximal subfield of $D$ has dimension $n$ and splits $D$. Conversely, it follows from Theorem 4.4 that every field which splits $D$ has degree divisible by $n$. We state this interesting fact as :

**Corollary 4.7** *If $D$ is a central division $k$-algebra of dimension $n^2$, and if $K$ splits $D$, then $n|[K : k]$.*

# Factor Sets and Crossed Product Algebras

In this section we introduce the notions of factor sets and crossed product algebras. These concepts will prove useful in analyzing the structure of central simple algebras, and will provide us with a more concrete description of elements of $Br(K/k)$ than we have seen so far. This description will allow us to make the connection between the relative Brauer group and the important concept of cohomology in the following section.

In the proof of the Frobenius Theorem, we determined the structure of a given division algebra $D$ by looking at a maximal subfield $K$ of $D$. In the case when $[D : K] = 2$, $K$ could be identified with $\mathbf{C}$, and the Skolem-Noether Theorem was applied to show the existence of $j \in D$ with

$$jzj^{-1} = \bar{z} \qquad \text{for all } z \in \mathbf{C}$$

which was the main step in showing that $D$ must be the quaternions.

More generally, suppose that $S$ is a central simple $k$-algebra of dimension $n^2$ which contains $K$ as a maximal subfield, $K/k$ is a field extension of degree $n$, and $G$ is the Galois group of $K$ over $k$. We shall now employ a method similar to the one we used in the proof of the Frobenius Theorem in order to analyze the structure of $S$. Instead of looking at a maximal subfield of $S$, we look at a field $K$ which splits $S$. Unfortunately, $S$ does not necessarily contain $K$, so we will have to choose a particular representative of $[S] \in Br(K/k)$ which contains $K$ as a maximal subfield. The details in the general case will be more complicated than in the Frobenius Theorem, for there are usually more than 2 automorphisms of $K$, and also because the base field is not always as nice as $\mathbf{R}$.

For any $\sigma \in G$, there exists $x_\sigma \in S$ such that

$$x_\sigma a x_\sigma^{-1} = \sigma(a) \qquad \text{for all } a \in K \tag{4.1}$$

by the Skolem-Noether Theorem. Note that $x_\sigma$ is unique up to scalar multiplication by non-zero elements of $K$; for if both $x'_\sigma$ and $x_\sigma$ satisfy (4.1), then $x'_\sigma x_\sigma^{-1}$ induces the identity on $K$, and is thus contained in $C(K) = K$. From this fact it follows that

$$x_\sigma x_\tau = a_{\sigma,\tau} x_{\sigma\tau} \qquad \text{for some } a_{\sigma,\tau} \in K^*.$$

The collection $\{a_{\sigma,\tau}\}$ is called a **factor set** of $S$ relative to $K$. It is useful to view $\{x_\sigma\}$ as a function $G \longrightarrow K^*$, and a factor set $\{a_{\sigma,\tau}\}$ as a function $G \times G \longrightarrow K^*$.

**Note:** We abbreviate $\{x_\sigma : \sigma \in G\}$ and $\{a_{\sigma,\tau} : \sigma, \tau \in G\}$ to $\{x_\sigma\}$ and $\{a_{\sigma,\tau}\}$.

Since the $x_\sigma$'s are unique only up to scalar multiplication, different choices of $\{x_\sigma\}$ will give rise to distinct factor sets. There is, however, a relationship between factor sets that are obtained by different choices for the $x_\sigma$'s. More precisely, suppose we have $\{x_\sigma\}$ and $\{x'_\sigma\}$ with factor sets $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$, respectively. Then $x'_\sigma x_\sigma^{-1} = f_\sigma$ for some $f_\sigma \in K^*$; that is,

$$x'_\sigma = f_\sigma x_\sigma \tag{4.2}$$

and we have

$$\begin{aligned} x'_\sigma x'_\tau &= f_\sigma x_\sigma f_\tau x_\tau && \text{by equation 4.2} \\ b_{\sigma,\tau} x'_{\sigma,\tau} &= f_\sigma \sigma(f_\tau) x_\sigma x_\tau && \text{by (4.2),(4.1), and definition of } b_{\sigma,\tau} \\ b_{\sigma,\tau} f_{\sigma\tau} x_{\sigma\tau} &= f_\sigma \sigma(f_\tau) a_{\sigma,\tau} x_{\sigma\tau} && \text{by equation 4.2} \end{aligned}$$

and so

$$b_{\sigma,\tau} f_{\sigma\tau} = f_\sigma \sigma(f_\tau) a_{\sigma,\tau}$$

Thus we obtain the following relationship between the two factor sets :

$$b_{\sigma,\tau} = \frac{f_\sigma \sigma(f_\tau)}{f_{\sigma\tau}} a_{\sigma,\tau}$$

This relationship will be useful in later discussions. Note that if we choose $x_1 = 1$, then $a_{1,\sigma} = a_{\sigma,1} = 1$ for all $\sigma \in G$. We call such a factor set **normalized.**

Although infinitely many bases for $\mathbf{C}$ over $\mathbf{R}$ exist, choosing the basis $\{1, i\}$ makes formulas easier to understand. We shall now show that the

$x_\sigma$'s form a basis for the algebra $S$ over the field $K$. The point is that $\{x_\sigma\}$ give multiplication formulas which take a particularly nice form, which in some sense makes the algebra look like a "twisted" group algebra. By choosing this basis in such a reasonable way, we will re-discover the algebraic definition of cohomology.

**Proposition 4.8** *$\{x_\sigma : \sigma \in G\}$ is a basis for $S$ over $K$.*

**Proof:** Since $|G| = [K : k] = [S : K]$, we need only show independence. So assume that the set is not independent, and choose a subset $J$ which is maximal with respect to the property that $J \subsetneq G$ and $\{x_\tau : \tau \in J\}$ is independent. Assume $\sigma \notin J$. Then

$$x_\sigma = \sum_{\tau \in J} \alpha_\tau x_\tau \qquad \text{for } \alpha_\tau \in K. \tag{4.3}$$

multiplying by any $r \in K$ gives

$$x_\sigma \cdot r = \sum_{\tau \in J} \alpha_\tau x_\tau \cdot r$$

yielding by (4.1)

$$\sigma(r) x_\sigma = \sum_{\tau \in J} \alpha_\tau \tau(r) x_\tau \qquad \text{for all } r \in K \tag{4.4}$$

Multiplying (4.3) by $\sigma(r)$ and using (4.1) to equate it with (4.4) gives

$$\alpha_\tau \tau(r) = \sigma(r) \alpha_\tau \qquad \text{for all } \tau \in J, r \in K.$$

Since $x_\sigma \neq 0$, there exists some $\tau \in J$ with $\alpha_\tau \neq 0$, so $\tau(r) = \sigma(r)$ for all $r \in K$, and so $\sigma = \tau \in J$, contradicting the choice of $\sigma$. Thus $J$ is all of $G$, and we are done. □

This proposition shows that, additively,

$$S = \bigoplus_{\sigma \in G} K x_\sigma$$

with multiplication characterized by

$$x_\sigma \alpha = \sigma(\alpha) x_\sigma \qquad \text{for all } \alpha \in K$$

$$\text{and} \quad x_\sigma x_\tau = a_{\sigma,\tau} x_{\sigma\tau}$$

It is natural to ask whether any function $\{a_{\sigma,\tau}\} : G \times G \longrightarrow K^*$ is the factor set for some algebra relative to some field. $\{a_{\sigma,\tau}\}$ cannot be arbitrary, since the associativity relation $x_\rho(x_\sigma x_\tau) = (x_\rho x_\sigma) x_\tau$ implies that

$$x_\rho a_{\sigma,\tau} x_{\sigma\tau} = a_{\rho,\sigma} x_{\rho\sigma} x_\tau$$

and so

$$\rho(a_{\sigma,\tau}) a_{\rho,\sigma\tau} x_{\rho\sigma\tau} = a_{\rho,\sigma} a_{\rho\sigma,\tau} x_{\rho\sigma\tau}$$

thus giving the constraint

$$\rho(a_{\sigma,\tau}) a_{\rho,\sigma\tau} = a_{\rho,\sigma} a_{\rho\sigma,\tau} \qquad (*).$$

This is, however, the only condition on $\{a_{\alpha,\tau}\}$ in order for it to be a factor set :

**Proposition 4.9** *Given an extension $K/k$, any set of elements $\{a_{\sigma,\tau}\}$ of $K$ satisfying (*) for all $\rho, \sigma, \tau \in G$ is the factor set relative to $K$ of a central simple $k$-algebra $A$. Further, $A$ contains $K$ as a maximal subfield.*

**Note:** In light of this proposition, any set of elements $\{a_{\sigma,\tau}\}$ of $K$ which satisfy (*) will be called a **factor set** (relative to $K$), regardless of whether or not an algebra of which $\{a_{\sigma,\tau}\}$ is a factor set is given.

**Proof:** Let $A$ be a vector space over $K$ with basis $\{e_\sigma : \sigma \in G\}$. Define multiplication via

$$(\alpha e_\sigma)(\beta e_\tau) = \alpha\sigma(\beta) a_{\sigma,\tau} e_{\sigma\tau}$$

and extend this definition to all of $A$ by linearity. Then it is easy to check that the axioms for an algebra hold in $A$ with $a_{1,1}^{-1} e_1$ being the identity element. For example, the distributive law holds (almost) by definition, and to show that $a_{1,1}^{-1} e_1$ is the identity element, we first note that for any $\sigma$,

$$1(a_{1,\sigma}) a_{1,\sigma} = a_{1,1} a_{1,\sigma}$$

since $\{a_{\sigma,\tau}\}$ satisfies (*). Thus $a_{1,1} = a_{1,\sigma}$, which implies that

$$\begin{aligned}(a_{1,1}^{-1} e_1) e_\sigma &= a_{1,1}^{-1} a_{1,\sigma} e_\sigma \\ &= e_\sigma.\end{aligned}$$

Similarly, it is easy to check that $\sigma(a_{1,1}) = a_{\sigma,1}$, which implies that

$$\begin{aligned}e_\sigma (a_{1,1}^{-1}) e_1 &= \sigma(a_{1,1}^{-1}) a_{\sigma,1} e_\sigma \\ &= e_\sigma\end{aligned}$$

showing that $a_{1,1}^{-1}e_1$ acts as identity element. $K$ is a subring of $A$ via the map

$$K \longrightarrow A$$

$$a \longmapsto a \cdot 1 \quad (1 = a_{1,1}^{-1}e_1).$$

To show that $K$ is its own centralizer, note that $\sum a_\sigma e_\sigma$ is contained in $C(K)$ if and only if

$$a(\sum a_\sigma e_\sigma) = (\sum a_\sigma e_\sigma)a \qquad \text{for all } a \in K,$$

which is equivalent to

$$aa_\sigma = a_\sigma \sigma(a) \qquad \text{for all } a \in K.$$

If $a_\sigma \neq 0$, this implies that $a = \sigma(a)$ for all $a \in K$, i.e., $\sigma$ is the identity. Thus $a_\sigma = 0$ if $\sigma$ is not the identity, and so $C(K) \subseteq K$. Since $K$ is clearly contained in $C(K)$, we have $K = C(K)$ in $A$. A similar argument shows that $k = C(A)$.

To see that $A$ is simple, suppose that $I$ is a proper two-sided ideal of $A$. Then $K \longrightarrow A/I$ is an injection. Let $\bar{e}_\sigma$ denote the image of $e_\sigma$ under this injection. Then $\bar{e}_\sigma a = a\bar{e}_\sigma$ for all $a \in k$. The proof that $\{e_\sigma : \sigma \in G\}$ are independent still works for $\{\bar{e}_\sigma : \sigma \in G\}$. Hence $I = 0$ and $A$ is simple. □

**Definition:** With notation as in the above proposition, $A$ is called the **crossed product** of $K$ and $G$ relative to the factor set $\{a_{\sigma,\tau}\}$, and is sometimes referred to simply as the **crossed product algebra** $(K, G, a)$.

In this terminology, Proposition 4.9 shows that any factor set $\{a_{\sigma,\tau}\}$ is the factor set of the central simple algebra $(K, G, a)$, and that $(K, G, a)$ contains $K$ as a maximal subfield.

Recall that a factor set $\{a_{\sigma,\tau}\}$ of an algebra is not uniquely determined, for $x_\sigma$ is unique only up to multiplication by non-zero scalars; that is, different choices for the $x_\sigma$'s will give rise to distinct factor sets $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$. As shown on page 118, however, such factor sets are related by

$$b_{\sigma,\tau} = \frac{f_\sigma \sigma(f_\tau)}{f_{\sigma\tau}} \cdot a_{\sigma,\tau} \qquad (**)$$

for some $f_\sigma \in K^*$ (recall that $\{b_{\sigma,\tau}\}$ arise from $\{x'_\sigma\}$, where $x'_\sigma = f_\sigma x_\sigma$). Conversely, given two factor sets $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$ which are related by (**), it is easy to check (using (*) and (**)) that the vector space map

$$(K, G, b) \longrightarrow (K, G, a)$$

$$x'_\sigma \longmapsto f_\sigma x_\sigma$$

is a $k$-algebra isomorphism. In short,

*Two factor sets which are related by (**) give rise to isomorphic crossed product algebras.*

We shall now show how factor sets and crossed product algebras relate to the relative Brauer group. In particular, the following theorem will show that every element in the Brauer group is $[(K, G, a)]$ for some factor set $\{a_{\sigma,\tau}\}$, and that one may associate an equivalence class of factor sets to each element of $Br(K/k)$. This gives a more concrete description of elements of $Br(K/k)$, which will actually make it possible to do some computations as well as relate the relative Brauer group to cohomology.

**Theorem 4.10** *Let $K/k$ be a Galois extension with Galois group $G$. Then there is a one-to-one correspondence between elements of $Br(K/k)$ and equivalence classes of factor sets $\{a_{\sigma,\tau}\}$ (relative to $K$), where $\{a_{\sigma,\tau}\} \sim \{b_{\sigma,\tau}\}$ if there exists $\{f_\sigma\}$ such that (**) holds.*

**Proof:** Given $x \in Br(K/k)$, Theorem 4.4 shows that there exists a unique (up to isomorphism) central simple algebra $A$ with $[A] = x$ in which $K$ embeds as a maximal subfield, and in fact the embedding is unique up to isomorphism (by the Skolem-Noether Theorem). From the above discussion we see that different choices of $A$ as a representative of $x \in Br(K/k)$ will give rise to equivalent factor sets, and so we get a well-defined map

$$Br(K/k) \longrightarrow \text{equiv. classes of } \{a_{\sigma,\tau}\}$$

$$[A] \longmapsto (\text{factor set of } A \text{ relative to } K).$$

Conversely, given a factor set $\{a_{\sigma,\tau}\}$, Proposition 4.9 shows that there exists a central simple algebra $(K, G, a)$ which has the $\{a_{\sigma,\tau}\}$ as factor set. Since equivalent factor sets give rise to isomorphic algebras, we get a well-defined map

$$\text{equiv. classes of } \{a_{\sigma,\tau}\} \longrightarrow Br(K/k)$$

$$\{a_{\sigma,\tau}\} \longmapsto [(K, G, a)].$$

It is clear that composing the above two maps (in either order) gives the identity, and so $Br(K/k)$ is in one-to-one correspondence with the set of equivalence classes of factor sets $\{a_{\sigma,\tau}\}$. □

# A Homological Characterization of the Brauer Group

In this section we introduce the idea of cohomology as another point of view from which to study the Brauer group. The notion of group cohomology is useful in many other contexts, so we shall develop this material in a more general setting than will actually be used here, although this development is not really more difficult. We shall then apply the ideas of cohomology to the study of the Brauer group.

The cohomology groups of a group were first defined by Hopf in the early 1940's by means of algebraic topology, and were used to study the relationship between the homology and homotopy groups of spaces. The definition of $H^n(G, M)$ was algebraicized by Eilenberg-MacLane (and independently by Eckmann) in the course of the development of homological algebra. It was they who realized that many classical constructions, such as equivalence classes of factor sets, could be described as cohomology groups in dimensions 0,1,2, and 3. The cohomology of groups has many applications in both topology and algebra. Its study remains a very active area of research. A nice introduction to this theory can be found in K. Brown, *Cohomology of Groups.*

Now let us proceed with the Eilenberg-MacLane definition of the cohomology of a group. For any group $G$ and any abelian group $M$ on which $G$ acts, we define

$$C^0(G, M) = M$$

and, for $n \geq 1$, we define $C^n(G, M)$ to be the set of all functions from $G^n$ (the product of $G$ with itself $n$ times) to $M$, that is, let

$$C^n(G, M) = \{f | f : G^n \longrightarrow M\}.$$

Notice that $C^n(G, M)$ is an abelian group under pointwise addition of functions, with the zero function acting as identity. More precisely, if $f_1, f_2 \in C^n(G, M)$, then by definition

$$(f_1 + f_2)(g_1, \ldots, g_n) = f_1(g_1, \ldots, g_n) + f_2(g_1, \ldots, g_n)$$

and

$$0(g_1, \ldots, g_n) = 0.$$

Notice that $G$ acts on $C^n(G, M)$ via

$$(g \cdot f)(g_1, \ldots, g_n) = g \cdot f(g_1, \ldots, g_n).$$

The elements of $C^n(G, M)$ are called **$n$-cochains of $G$ with coefficients in $M$**, and $C^n(G, M)$ is called the **$n$-th cochain group**. We shall

now define, for each $n \geq 0$, a homomorphism which carries the group of $n$-cochains into the group of $n+1$ cochains. Let $\delta_0 : C^0(G,M) \longrightarrow C^1(G,M)$ be defined by

$$(\delta_0 f)(g_1) = g_1 \cdot f - f$$

for $f \in C^0(G,M)$, that is $f \in M$. For $n \geq 1$, define $\delta_n : C^n(G,M) \longrightarrow C^{n+1}(G,M)$ by

$$\begin{aligned}\delta_n(f)(g_1,\dots,g_{n+1}) = \quad & g_1 \cdot f(g_2,\dots,g_{n+1}) \\ & + \textstyle\sum_{i=1}^{n}(-1)^i f(g_1,\dots,g_{i-1},g_ig_{i+1},\dots,g_{n+1}) \\ & +(-1)^{n+1} f(g_1,\dots,g_n).\end{aligned}$$

So for $n = 1$ this map is defined by

$$\delta_1 f(g_1,g_2) = g_1 \cdot f(g_2) - f(g_1g_2) + f(g_1)$$

and for $n = 2$ we have

$$\delta_2 f(g_1,g_2,g_3) = g_1 \cdot f(g_2,g_3) - f(g_1g_2,g_3) + f(g_1,g_2g_3) - f(g_1,g_2).$$

$\delta_n$ is called the **$n$-th boundary map**. It is clear that each $\delta_n$ is a group homomorphism. The maps $\delta_n$ also have the following important property :

**Proposition 4.11** $\delta_{n+1} \circ \delta_n = 0$

**Proof:** This is an easy exercise which follows immediately from the definitions, and will be left to the reader. □

This proposition shows that $\{C^n, \delta_n\}$ forms a **cochain complex**; that is, a sequence of abelian groups $\{C^n\}$ and homomorphisms $\delta_n : C^n \longrightarrow C^{n+1}$ satisfying $\delta_{n+1} \circ \delta_n = 0$. In shorter form, we may write this cochain complex as

$$0 \longrightarrow C^0 \xrightarrow{\delta_0} C^1 \longrightarrow \cdots \longrightarrow C^n \xrightarrow{\delta_n} C^{n+1} \longrightarrow \cdots$$

Whenever one has a cochain complex, one may take its homology. We now proceed to do this. Let

$$\begin{aligned} Z^n &= kernel(\delta_n) \\ B^n &= image(\delta_{n-1}) \end{aligned}$$

Elements of $Z^n$ are called **$n$-cocycles**; elements of $B^n$ are called **$n$-coboundaries** . The property $\delta_{n+1} \circ \delta_n = 0$ tells us that $B^n \subseteq Z^n$. Since $Z^n$ is abelian, we may form the quotient $Z^n/B^n$. We define the **$n$-th cohomology group of $G$ with coefficients in $M$** to be

$$H^n(G, M) = Z^n/B^n$$

We shall now restrict our attention to the special case when $G = Gal(K/k)$ and $M = K^*$ for a galois extension $K/k$. The groups $H^n(G, K^*)$ are called the **Galois cohomology groups of the extension $K/k$ with coefficients in $K^*$** . As we shall now see, the machinery of cohomology captures the properties and relations between factor sets in a more manageable way.

In the terminology of the previous section, and letting $G = Gal(K/k)$, we can think of $\{f_\sigma\}$ as a function $G \longrightarrow K^*$ (i.e., a 1-cochain), and $\{a_{\sigma,\tau}\}$ as a function $G \times G \longrightarrow K^*$, (i.e., a 2-cochain). One version of Hilbert's famous "Theorem 90" states that $H^0(G, K^*) = k^*$ and $H^1(G, K^*) = 1$. An outline of the proof of this theorem is given in Exercise 41. We shall now concentrate on $H^2(G, K^*)$, and will "re-discover" the relationship between this group and the relative Brauer group $Br(K/k)$; namely, that they are isomorphic.

$Z^2$ consists of functions $a : G \times G \longrightarrow K^*$ such that $\delta_2(a) = 1$; that is (writing $K^*$ multiplicatively, of course)

$$1 = \delta_2(a)(\rho, \sigma, \tau) = \rho(a(\sigma, \tau))a(\rho\sigma, \tau)^{-1} \cdot a(\rho, \sigma\tau)a(\rho, \sigma)^{-1}$$

or, equivalently,

$$\rho(a(\sigma, \tau))a(\rho, \sigma\tau) = a(\rho, \sigma)a(\rho\sigma, \tau)$$

This condition is called the **cocycle condition** . The cocycle condition is just condition (*) on page 120. In other words, the 2-cocycles of $C^2(G, K^*)$ are just the factor sets relative to $K$.

$B^2$ consists of functions which are the image under $\delta_1$ of $f : G \longrightarrow K^*$; that is

$$\delta_1(f)(\sigma, \tau) = \sigma f(\tau) f(\sigma\tau)^{-1} f(\sigma)$$

Since two 2-cocycles represent the same element of $H^2(G, K^*)$ precisely when they differ (multiplicatively) by a 2-coboundary, we see that $H^2(G, K^*)$ consists of the set of factor sets (=2-cocycles) modulo the equivalence relation $a \sim b$ in $Z^2(G, K^*)$ if

$$b_{\sigma,\tau} = \frac{f_\sigma \sigma(f_\tau)}{f_{\sigma\tau}} \cdot a_{\sigma,\tau}$$

This is just condition (**) on page 121. But Theorem 4.10 shows that the set of factor sets modulo this equivalence relation is in one-to-one correspondence with $Br(K/k)$. Thus we see that, as sets, $Br(K/k)$ is in one-to-one correspondence with $H^2(G, K^*)$.

**Remark:** As we noted on page 118, every factor set (i.e., 2-cocycle) is equivalent to a normalized factor set. This shows that we may assume that every $a \in Z^2(G, K^*)$ satisfies $a(1, \sigma) = a(\sigma, 1) = 1$. This assumption often simplifies computations.

Our next goal is to prove that the above correspondence is an isomorphism of groups; that is, we shall prove that the map

$$\psi : H^2(G, K^*) \longrightarrow Br(K/k)$$

given by

$$\psi(a) = [(K, G, a)]$$

is an isomorphism, where $a$ is a 2-cocycle. The above discussion shows that $\psi$ is one-to-one and onto, so it remains only to see that $\psi$ is a homomorphism. In other words, we must prove the following

**Lemma 4.12** *If $K/k$ is a galois extension with Galois group $G$, and if $a$ and $b$ are factor sets, then*

$$[(K, G, a)][(K, G, b)] = [(K, G, ab)] \qquad \text{in } Br(K/k).$$

The following proof is due to Chase, and seems to be a quicker, more conceptual proof than is currently contained in the literature. For a more computational proof, see the exercises at the end of this chapter.

**Proof:** Let $A = (K, G, a), B = (K, G, b)$, and $C = (K, G, c)$, where $c = ab$. What we must show is that $A \otimes_k B$ is equivalent (as a finite-dimensional central simple algebra) to $C$. The idea of the proof is a slightly more involved version of a technique that has been used throughout this book : we just find an appropriate module on which both $A \otimes_k B$ and $C$ act (on opposite sides). From this we obtain a homomorphism of the first algebra into an endomorphism ring over the second, and conclude that this is an isomorphism by simplicity of $A \otimes_k B$ and counting dimensions. It will follow that the two algebras are equivalent in $Br(K/k)$.

With the above outline in mind, let $M = A^\circ \otimes_K B$, where we view $A$ and $B$ as $K$-modules via left multiplication. In $M$ we have that

$$xa \otimes_K b = a \otimes_K xb \qquad \text{for all } x \in K, a \in A, b \in B \tag{4.5}$$

where $\otimes_K$ denotes the tensor product of two elements over $K$. Note that the left-hand side of the equation is really $a \circ x \otimes_K b$, where $\circ$ denotes multiplication in $A^\circ$. The expression $a \circ x$ is, however, equal to $xa$, the multiplication here taking place in $A$. We shall continue to use this terminology without comment.

We may now make $M$ a right $A \otimes_k B$-module via right multiplication :

$$(a' \otimes_K b')(a \otimes_k b) = a'a \otimes_K b'b \qquad \text{for all } a, a' \in A \text{ and } b, b' \in B.$$

The next step of the proof is to introduce a left $C$-module structure on $M$ which makes $M$ into a $C-(A \otimes_k B)$-bimodule.

Let $\{u_\sigma\}, \{v_\sigma\}, \{w_\sigma\}$ be the distinguished bases over $K$ of $A, B$, and $C$, respectively (see the proof of Proposition 4.9). Define the operation of $C$ on $M$ on the left by

$$(xw_\sigma)(a \otimes_K b) = xu_\sigma a \otimes_K v_\sigma b \qquad \text{for all } x \in K, \sigma \in G, a \in A, b \in B \quad (4.6)$$

It is not difficult to check that this operation is well-defined, and that $M$ then satisfies the axioms of a (left) $C$-module, and that this structure is compatible with the right $A \otimes_k B$-module structure on $M$. Hence $M$ has a $C-(A \otimes_k B)$-bimodule. We shall give what is perhaps the most crucial of these computations; namely, the verification of the associativity formula

$$(cc')m = c(c'm) \qquad \text{for } c, c' \in C, m \in M.$$

So assume $c = xw_\sigma, c' = x'w_\tau$, and $m = a \otimes_K b$ with $x, x' \in K, \sigma, \tau \in G$, and $a \in A, b \in B$. Then

$$\begin{aligned}
(cc')m &= x\sigma(x')a_{\sigma,\tau}b_{\sigma,\tau}u_{\sigma\tau}a \otimes_K v_{\sigma\tau}b && \text{by (4.6)}\\
&= x\sigma(x')a_{\sigma,\tau}u_{\sigma\tau}a \otimes_K b_{\sigma,\tau}v_{\sigma\tau}b && \text{by (4.5)}\\
&= x\sigma(x')u_\sigma u_\tau a \otimes_K v_\sigma v_\tau b\\
&= xu_\sigma x'u_\tau a \otimes_K v_\sigma v_\tau b\\
&= xw_\sigma(x'u_\tau a \otimes_K v_\tau b) && \text{by (4.6)}\\
&= c(c'm) && \text{by (4.6)}
\end{aligned}$$

The $C-(A \otimes_k B)$-bimodule structure of $M$ gives a $k$-algebra homomorphism

$$\begin{aligned} (A \otimes_k B)^\circ &\longrightarrow End_C(M) \\ x &\longmapsto f_x \end{aligned} \qquad (4.7)$$

where $f_x(m) = mx$. This homomorphism is injective since $A \otimes_k B$ (and thus $(A \otimes_k B)^\circ$is a simple algebra. Thus it suffices to show that both the range and domain have the same $k$-dimension in order to prove that the above map is an isomorphism.

Let $n = [K : k]$. Since $A, B$, and $C$ each have dimension $n$ over $K$, $M$ has dimension $n^2$ over $K$, and so

$$[M : k] = n^2[K : k] = n^3 = n[C : k].$$

Since a finitely generated module over a simple algebra is determined (up to isomorphism) by its dimension over the base field, it follows that $M$ is a free $C$-module of rank $n$, $M \approx C^n$. Thus

$$End_C(M) \approx End_C(C^n) \approx \mathcal{M}_n(End_C(C)) \approx \mathcal{M}_n(C^\circ) \approx C^\circ \otimes_k \mathcal{M}_n(k).$$

It follows that

$$dim_k(End_C(M)) = n^2 dim_k(C) = n^4 = dim_k(A \otimes_k B).$$

Thus the homomorphism in (4.7) is an isomorphism, so $(A \otimes_k B)^\circ \approx C^\circ \otimes_k \mathcal{M}_n(k)$, and so $(A \otimes_k B)^\circ \sim C^\circ$. It follows that $A \otimes_k B \sim C$ and we are done. □

Lemma 4.12 thus shows that the map $\psi : H^2(G, K^*) \longrightarrow Br(K/k)$ is a homomorphism, and the previous discussion shows that $\psi$ is an isomorphism. This gives us another way of looking at the Brauer group, and connects this group to many other important areas of mathematics. We state this as a theorem for emphasis.

**Theorem 4.13** *For a galois extension $K/k$, $Br(K/k) \approx H^2(Gal(K/k), K^*)$ as groups.*

## The Brauer Group is Torsion

Using the fact that, for galois extensions, the relative Brauer group $Br(K/k)$ is isomorphic to the cohomology group $H^2(Gal(K/k), K^*)$, we may deduce facts about relative Brauer groups from general properties of cohomology groups. In this section we shall prove that the Brauer group is a torsion group; that is, each element of $Br(k)$ has finite order. Although this proof can be carried out directly in the Brauer group, it becomes easier to understand when placed in the context of homological algebra. We now begin with a standard result about the cohomology of finite groups.

**Theorem 4.14** *If $G$ is a finite group, then $|G|H^n(G, M) = 0$.*

**Proof:** We shall prove this fact in the case $n = 2$. The more general case is similar, and will be left as an exercise.

Let $f \in Z^2(G, M)$, so $\delta_2 f = 0$; that is

$$0 = (\delta_2 f)(g_1, g_2, g_3) = g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2).$$

In other words

$$f(g_1, g_2) = g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3).$$

Summing over all $g_3 \in G$ gives

$$|G| f(g_1, g_2) = \sum_{g_3 \in G} (g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3)).$$

Now let $h(g_2) = \sum_{g_3 \in G} f(g_2, g_3)$. Note that

$$\sum_{g_3 \in G} f(g_1, g_2 g_3) = \sum_{g_3 \in G} f(g_1, g_3)$$

and so

$$\begin{aligned} |G| f(g_1, g_2) &= g_1 h(g_2) - h(g_1 g_2) + h(g_1) \\ &= (\delta_1 h)(g_1, g_2) \in B^2(G, M). \end{aligned}$$

This shows that $|G| Z^2(G, M) \subseteq B^2(G, M)$ and thus $|G| H^2(G, M) = 0$. □

This theorem may now be used to show that the Brauer group is a torsion group.

**Corollary 4.15** *For any field $k$, $Br(k)$ is a torsion abelian group.*

**Proof:** Corollary 4.6 shows that $Br(k) = \bigcup Br(K/k)$, where the union is taken over all galois extensions $K/k$. But $Br(K/k) \approx H^2(G, K^*)$, which by the above theorem is annihilated by $|G| = [K : k]$. □

This corollary also shows how the reduction of questions about $Br(k)$ to properties of relative Brauer groups $Br(K/k)$ for galois extensions $K/k$ can be a useful technique.

# A Primary Decomposition Theorem for Central Division Algebras

The fact that the Brauer group is a torsion abelian group tells us a great deal about central division algebras. This harkens back to the comment at the beginning of this chapter that statements about the group structure of $Br(k)$ can be used to give us concrete information about a single central division algebra.

Given a central division algebra $D$ over $k$, the previous section shows that $[D]$ has finite order in $Br(k)$, so this order can be written as a product

of powers of distinct primes. It would be nice if $D$ itself could be broken up into pieces corresponding to this prime factorization. The main goal of this section is to prove such a theorem. Along the way we will learn about a variety of dimensionality relationships among various algebras.

We begin by recalling a few definitions. Let $D$ be a central division algebra over $k$, and let $K$ be a splitting field for $D$; i.e., $D_K \approx \mathcal{M}_n(K)$ for some $n$. We defined the **degree** of $D$, denoted $deg(D)$, to be $n$. Note that since $[D:k][K:k] = n^2[K:k]$, $[D:k] = n^2$, and so the degree of $D$ over $k$ may also be defined as the square root of the dimension of $D$ as a vector space over $k$. If $A$ is a central simple $k$-algebra, then $A \approx \mathcal{M}_m(D)$ for a unique division algebra $D$, and we define the **(Schur) index** of $A$, denoted $ind(A)$ , to be the degree of $D$. The degree and the index of a division algebra are equal by definition. Finally, we define the **exponent** of the central simple $k$-algebra $A$, denoted $exp(A)$, to be the order of $[A]$ in $Br(k)$; that is, $exp(A)$ is the smallest number $m$ so that $A^{\otimes m} \approx \mathcal{M}_r(k)$ for some $r$, where $A^{\otimes m}$ denotes the tensor product of $m$ copies of $A$.

Although it is not obvious from the definitions, there is a relationship between the exponent and the index of a central simple algebra; namely, the former divides the latter. We state this as

**Proposition 4.16** $[A]^{ind(A)} = 1$ *in* $Br(k)$; *that is,* $exp(A)$ *divides* $ind(A)$.

**Proof:** $A \approx \mathcal{M}_r(D)$ for some central division algebra $D$ over $k$ with $[D:k] = m^2$, where $m = ind(A)$. By Corollary 4.5, there is a finite galois extension $K$ of $k$ which is a splitting field for $D$. Let $G$ be the Galois group of $K$ over $k$, and $|G| = n = [K:k]$. By Theorem 4.4, $[A:k] = n^2$. Note that, since $A \approx \mathcal{M}_r(D)$, we have $n^2 = r^2[D:k] = r^2m^2$, so $n = rm$.

Now $[A] = [(K,G,a)]$ for some $a \in Z^2(G,K^*)$. Since $[A]^m = [(K,G,a)]^m$, it suffices to show that $a^m \in B^2(G,K^*)$. Let $V = D^r$, and note that $V$ is a left $End_D(V)$-module, where the action is given by $\phi \cdot v = \phi(v)$ for $\phi \in End_D(V), v \in V$. Since $A \approx \mathcal{M}_r(D) \approx End_D(V)$, we see that $V$ is a left $A$-module. Since $K \subset A$, $V$ is a vector space over $K$. Let's compute it's dimension. We have

$$rm^2 = [V:D][D:k] = V:k] = [V:K][K:k] = [V:K]rm$$

and so $[V:K] = m$. Choose a basis $\{v_1, \ldots, v_m\}$ for $V$ over $K$. Since $V$ is a left $A$-module, we know that for each $c \in A$, $c \cdot v_i = \sum_{j=1}^{m} c_{ij}v_j$ with $c_{ij} \in K$. We think of the $c_{ij}$ as an $m \times m$ matrix via

$$c \cdot [v] = [c_{ij}][v] \quad \text{with } [v] = \begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix}$$

Now choose a basis $\{x_\sigma\}_{\sigma\in G}$ for $(K,G,a)$ over $K$, and let $X_\sigma \in \mathcal{M}_m(K)$ denote the matrix associated to $x_\sigma$. For $\sigma,\tau \in G$, let $\sigma(X_\tau)$ denote the matrix obtained from $X_\tau$ by letting $\sigma$ act on each entry. Then

$$x_\sigma x_\tau \cdot [v] = x_\sigma X_\tau[v] = \sigma(X_\tau)X_\sigma[v]$$

and

$$x_\sigma x_\tau \cdot [v] = a_{\sigma,\tau}x_{\sigma\tau} \cdot [v] = a_{\sigma,\tau}X_{\sigma\tau}[v].$$

Thus

$$a_{\sigma,\tau}X_{\sigma\tau} = \sigma(X_\tau)X_\sigma.$$

Taking the determinant of both sides of this last equation, we see that

$$a^m_{\sigma,\tau}det(X_{\sigma\tau}) = \sigma(det(X_\tau))det(X_\sigma)$$

with $det(X_\sigma) \in K^*$. Thus $a^m \in B^2(G,K^*)$ and we are done. □

Note that Proposition 4.16 provides another proof that $Br(k)$ is a torsion group.

Before proving the main theorem of this section, we need two lemmas. The following lemma gives a sort of partial converse to Proposition 4.16. Taken together, the two statements show that $exp(A)$ and $ind(A)$ have the same prime factors.

**Lemma 4.17** *Every prime divisor of $ind(A)$ is a prime divisor of $exp(A)$.*

The following proof gives another example of the technique of extension of scalars, a common tool in studying the Brauer group.

**Proof:** Let $(K,G,a) \approx \mathcal{M}_m(D)$ be a crossed product algebra with $[A] = [(K,G,a)] = [\mathcal{M}_m(D)]$, where $D$ is a central division $k$-algebra, and let $d = ind(A) = ind(D) = deg(D)$. Let $p$ be a prime dividing $d$. Note that $|G|^2 = [(K,G,a) : k] = m^2d^2$; hence $|G| = md$ and $p$ divides $|G|$. Let $G_p$ denote the $p$-Sylow subgroup of $G$, say $|G_p| = p^r$, and let $K_p \supset K$ denote the fixed field of $G_p$. Then $[K : K_p] = p^r$ by the Fundamental Theorem of Galois Theory. Since $G_p$ is $p$-Sylow, $p \not| [K_p : k]$, and so $K_p$ cannot split $A$ by Corollary 4.7. By the given, $p$ divides the degree of any maximal subfield of $D$, so $exp(A_{K_p}) \neq 1$. But $(A \otimes_k K_p) \otimes_{K_p} K = A \otimes_k K$ splits and $[K : K_p] = p^r$, so $p$ divides $exp(A_{K_p})$.

Recall that there is a homomorphism

$$Br(k) \longrightarrow Br(K_p)$$

$$[S] \longmapsto [S_{K_p}]$$

given by extension of scalars. Since this map is a homomorphism of groups it is clear that $exp(A_{K_p})$ divides $exp(A)$ and we are done. □

The tensor product of two division algebras is not always a division algebra. This is the reason that division algebras were not used as elements of the Brauer group. The following lemma gives a sufficient condition for the product of two division algebras to be a division algebra.

**Lemma 4.18** *If $D_1$ and $D_2$ are central division algebras with $deg(D_1)$ and $deg(D_2)$ relatively prime, then $D_1 \otimes D_2$ is a division algebra.*

**Proof:** $D_1 \otimes D_2 \approx \mathcal{M}_m(D)$ for some central division algebra $D$ and some $m$; we will show that $m = 1$. Well, $D_1^\circ \otimes D_1 \approx \mathcal{M}_n(k)$, where $k$ is the base field. Then

$$n^2 = [\mathcal{M}_n(k) : k] = [D_1^\circ \otimes D_1 : k] = [D_1 : k][D_1 : k]$$

and so $n = [D_1 : k]$. Now

$$\begin{aligned} \mathcal{M}_n(D_2) &= \mathcal{M}_n(k) \otimes D_2 \\ &= D_1^\circ \otimes D_1 \otimes D_2 \\ &= D_1^\circ \otimes \mathcal{M}_m(D) \\ &= \mathcal{M}_m(D_1^\circ \otimes D) \\ &= \mathcal{M}_m(\mathcal{M}_r(D')) \quad \text{for some division algebra } D' \\ &= \mathcal{M}_{mr}(D'). \end{aligned}$$

So $n = mr$, which implies that $m$ divides $[D_1 : k]$. Similarly, $m$ divides $[D_2 : k]$. Since the degrees of $D_1$ and $D_2$ are relatively prime, and hence $[D_1 : k]$ and $[D_2 : k]$ are relatively prime, it follows that $m = 1$. □

We are now ready to prove a nice decomposition theorem for central division algebras. This theorem is analogous to the primary decomposition theorem for finitely generated modules over a principal ideal domain. In each case we break down the given module (or division algebra) into its so-called "primary components".

**Theorem 4.19** *Let $D$ be a finite-dimensional central division algebra over $k$, and $deg(D) = p_1^{n_1} \cdots p_r^{n_r}$, where $p_1, \dots, p_r$ are distinct primes. Then there is a unique (up to isomorphism) decomposition*

$$D = D_1 \otimes D_2 \otimes \cdots \otimes D_r$$

*where $D_i$ are division algebras and $ind(D_i) = p_i^{n_i}$.*

**Proof:** It suffices to show that, if $deg(D) = n = n_1 n_2$ with $n_1$ and $n_2$ relatively prime, then $D \approx D_1 \otimes D_2$, where $deg(D_1) = n_1$ and $deg(D_2) = n_2$. The theorem will then follow by induction on the number of distinct

primes in the factorization of $n$. Since $n_1$ and $n_2$ are relatively prime, there are integers $u, v$ with $un_1 + vn_2 = 1$. Let $D_1, D_2$ be the unique central division algebras such that $[D_1] = [D]^{vn_2}$ and $[D_2] = [D]^{un_1}$. Then $[D_1 \otimes D_2] = [D]^{(un_1+vn_2)} = [D]$. We also know that $[D_1]^{n_1} = [D]^{vn} = [k]$ by Proposition 4.16 (recall that $deg(D_1) = ind(D_1)$ since $D_1$ is a division algebra); hence $exp(D_1) \mid n_1$. Similarly, $exp(D_2) \mid n_2$. Lemma 4.17 implies that $exp(D_i)$ and $deg(D_i)$ $(i = 1, 2)$ have the same prime divisors, and $(n_1, n_2) = 1$ by the given, hence $(deg(D_1), deg(D_2)) = 1$. Since $D_1$ and $D_2$ are division algebras of relatively prime degree, $D_1 \otimes D_2$ is a division algebra by Lemma 4.18. Thus $[D_1 \otimes D_2] = [D]$ implies that $deg(D_1 \otimes D_2) = deg(D)$. It follows that $deg(D_i) = n_i, i = 1, 2$. □

In view of this theorem, the structure theory of division algebras reduces to the case where the degree is a prime power.

## Summary

In this chapter we studied the Brauer group $Br(k)$ of a field $k$, which consists of all of the isomorphism classes of central simple $k$-algebras under the equivalence relation given on page 110. $Br(k)$ is a group under the operation of tensor product, with $[\mathcal{M}_n(k)] = [k]$ acting as identity element and $[A^\circ]$ acting as the inverse of $[A]$. $Br(k)$ acts as a "classifier" of central division algebras, and in the exercises we will get a glimpse of the connection of the Brauer group with many other areas of algebra and number theory.

The study of $Br(k)$ was reduced to the study of $Br(K/k)$ for galois extensions $K/k$. Using factor sets, which involves ideas generalizing those used in the proof of the Frobenius Theorem, we obtained more explicit information on elements of $Br(K/k)$. The somewhat messy calculations with factor sets gave the impetus for our re-discovery of the powerful homological viewpoint. The concrete connection of the cohomology of groups with the theory of central simple algebras culminated in the proof that $Br(K/k) \approx H^2(Gal(K/k), K^*)$. Using this isomorphism, we proved that $Br(k)$ is a torsion abelian group. Finally, we used group theoretic facts about $Br(k)$ to give information about the indices and exponents of central simple algebras, and to prove a structure theorem on central division algebras, re-emphasizing the usefulness of making the set of (equivalence classes of) finite-dimensional central simple algebras into a group.

## Exercises

1. Show that the four conditions given on page 110 for two algebras to be similar are indeed equivalent.

2. Let $A = [a_{ij}] \in \mathcal{M}_n(k)$ and $B = [b_{kl}] \in \mathcal{M}_m(k)$. The **Kronecker product of matrices** $A$ and $B$, denoted by $A \otimes B$, is the $nm \times nm$ block matrix $[Ab_{kl}], 1 \leq k, l \leq m$. Prove that the mapping

$$\mathcal{M}_n(k) \otimes \mathcal{M}_m(k) \longrightarrow \mathcal{M}_{nm}(k)$$

$$(A, B) \longmapsto A \otimes B$$

induces a $k$-algebra isomorphism.

3. Show that the set of isomorphism classes of finite-dimensional algebras over a given field $k$ actually forms a set. Estimate its cardinality.

4. (a) Show that $Br(\ )$ is a functor from the category of fields and field homomorphisms to the category of abelian groups and group homomorphisms (if you don't know what these words mean, look them up).

   (b) Let $i : k \longrightarrow K$ and $j : k \longrightarrow K$ be homomorphisms of fields and let $i_*$ and $j_*$ be the induced maps from $Br(k)$ to $Br(K)$. Let $F = \{x \in k : i(x) = j(x)\}$, and assume that $K/i(F)$ is a finite galois extension. Prove that $i_* = j_*$.

5. Give an example of two finite-dimensional central division algebras over $k$ whose tensor product (over $k$) is *not* a division algebra.

6. (a) Prove that $Br(k) = 0$ for any algebraic extension of a finite field.

   (b) Prove that $Br(k) = 0$ for any field of transcendence degree one over an algebraically closed field.

7. (a) Show that a $k$-algebra $A$ is central simple over $k$ if and only if there is a $k$-algebra $B$ such that $A \otimes B \approx \mathcal{M}_n(k)$ as $k$-algebras for some $n$.

   (b) Let $A, A'$ be central simple $k$-algebras. Show that if $[A] = [A']$ in $Br(k)$ and $[A : k] = [A' : k]$, then $A \approx A'$ as $k$-algebras.

8. Theorem 4.4 may be interpreted as follows: Given $z \in Br(K/k)$, there is a pair $(S, i)$ such that $z = [S]$, where $S$ is a central simple $k$-algebra and $i : K \longrightarrow S$ is a $k$-algebra homomorphism whose image is a maximal commutative subalgebra of $S$. Suppose that $(S', i')$ is another such pair and $z = [S']$. Prove that there is a $k$-algebra isomorphism $\phi : S \longrightarrow S'$ such that $\phi i = i'$. [Hint: Use Exercise 7b and the Skolem-Noether Theorem.]

9. Let $A$ be a central simple algebra with maximal commutative subalgebra $K$. Assume that $K/k$ is galois with Galois group $G$. Let $E$ be the normalizer of $K^*$ in $A^*$. Find a homomorphism $\phi$ of $E$ onto $G$ such that $Ker(\phi) = K^*$. $E$ is an example of what is called a "group extension of $G$ by $K^*$".

10. Let $A$ be a central simple $k$-algebra containing a field $F$. Let $C(F)$ be the centralizer of $F$ in $A$. Show that the following equality holds in $Br(F)$: $[F \otimes_k A] = [C(F)]$. [Hint: Use the Double Centralizer Theorem.]

**Remark:** The interplay between simple subrings and their centralizers deserves to be understood; in this connection, see also Chapter 3, Exercise 3.16. In that case, the subalgebra was central simple but there was no hypothesis on the ambient algebra. In this situation, the ambient algebra is finite-dimensional central simple and the subalgebra (which doesn't need to be a field for most of the argument) is simple. In either case, what's involved is the structure theory of central simple algebras, the Centralizer Theorem and the Skolem-Noether Theorem.

### Schur Index

11. Let $A$ be a central simple $k$-algebra. Prove the following :

(a) If $[A : k] = n^2$, then $ind(A)|n$. $ind(A) = n$ if and only if $A$ is a division algebra.

(b) If $A'$ is a central simple $k$-algebra such that $[A] = [A']$ in $Br(k)$, then $ind(A') = ind(A)$.

(c) $A$ possesses a splitting field of degree $ind(A)$ over $k$.

(d) If $K$ is any splitting field of $A$ then $ind(A)|[K : k]$.

(e) $ind(A) = min\{[K : k] : K \text{ splits } A\}$.

(f) For $m \geq 1$, $ind(A \otimes \cdots \otimes A)$ (the tensor product of $m$ copies of $A$) divides $ind(A)$.

12. Let $A$ be a central simple $k$-algebra and let $K/k$ be a finite extension. Prove that

(a) $ind(A_K)|ind(A)$.

(b) $ind(A)|[K : k]ind(A_K)$.

(c) If $ind(A)$ and $[K : k]$ are relatively prime, then $ind(A_K) = ind(A)$; and if $A$ is also a division algebra, then so is $A_K$.

## Exponents

13. Let $A$ and $B$ be finite-dimensional central simple $k$-algebras. Let $K/k$ be a finite field extension. Prove the following facts :

    (a) If $[A] = [B]$, then $exp(A) = exp(B)$.

    (b) $exp(A_K) \mid exp(A)$.

    (c) $exp(A) \mid [K : k]exp(A_K)$.

    (d) If $ind(A)$ is relatively prime to $[K : k]$, then $exp(A_K) = exp(A)$.

    (e) $exp(A \otimes B)$ divides the least common multiple of $exp(A)$ and $exp(B)$.

    (f) $exp(A^{\otimes m}) = exp(A)/n$, where $n$ is the greatest common divisor of $m$ and $exp(A)$.

    (g) If $ind(A)$ and $ind(B)$ are relatively prime, then $ind(A \otimes B) = (ind(A))(ind(B))$ and $exp(A \otimes B) = (exp(A))(exp(B))$.

14. Let $A$ be a finite-dimensional central simple $k$-algebra with $ind(A) = p^j n$, where $p$ is prime, $j \geq 1$, and $p$ does not divide $n$. Prove that there is a field extension $K$ over $k$ whose dimension is relatively prime to $p$, for which $ind(A_K) = p^j$.

## Generalized Quaternion Algebras

Let $k$ be a field of characteristic not equal to 2. For $a, b \in k^*$ let $\left(\frac{a,b}{k}\right)$ denote the vector space of dimension 4 over $k$ having the elements $1, i, j, k$ as a basis. Defining $i^2 = a, j^2 = b$ and $ij = -ji = k$ makes this into a $k$-algebra (don't confuse the field $k$ with the element $k$; both used because that is the standard notation). Note that $k^2 = -ab, ki = -ik = -aj$, and $jk = -kj = -bi$. The algebra $\left(\frac{a,b}{k}\right)$ is called a **generalized quaternion algebra** .

15. (a) Show that every 4-dimensional central simple algebra over $k$ is isomorphic to $\left(\frac{a,b}{k}\right)$ for some $a, b \in k^*$. [Hint: See the proof of the Frobenius Theorem.]

    (b) Using this description of the central simple algebra, explicitly give its factor set.

16. Show that $\left(\frac{1,1}{k}\right) \approx \mathcal{M}_2(k)$. [Hint: Consider the matrices $e_{12} + e_{21}$ and $e_{11} - e_{22}$.]

17. Show that $\left(\frac{a,b}{k}\right) \approx \left(\frac{b,a}{k}\right)$.

18. Show that $\left(\frac{a,b}{k}\right) \approx \left(\frac{ax^2, by^2}{k}\right)$ for $x, y \in k^*$. [Hint: Remember the proof of the Frobenius Theorem.]

19. Show that $\left(\frac{a,b}{k}\right) \otimes_k K \approx \left(\frac{a,b}{K}\right)$ for field $K \supseteq k$.

20. Show that $\left(\frac{a,b}{k}\right)$ is a central simple $k$-algebra. [Hint: Compute the center. Tensor with the algebraic closure and apply previous results for the other part.]

21. Show that $\left(\frac{a, 1-a}{k}\right) \approx \mathcal{M}_2(k)$. [Hint: Define the quaternion conjugate of $z = u + iv + jw + kx$ to be $\bar{z} = u - iv - jw - kx$. Define $N(z) = \bar{z}z = z\bar{z}$. $N(z)$ is called the **(quaternion) norm** of $z$. Show that an element has an inverse if and only if $N(z) \neq 0$. Do this by observing that the regular representation has determinant equal to the square of $N$. Now compute $N(1 + i + j)$.]

22. Show that $\left(\frac{1,b}{k}\right) \approx \left(\frac{a,-a}{k}\right) \approx \mathcal{M}_2(k)$. [Hint: Consider $j + k$ and $i + j$.]

23. Show that $\left(\frac{a,b}{k}\right)$ is isomorphic to its opposite algebra.

This shows that each quaternion algebra $\left(\frac{a,b}{k}\right)$ has order dividing 2 in $Br(k)$. If it is a division ring, it has order 2. A long standing conjecture was that these elements generate the part of the Brauer group annihilated by 2. This was eventually proved by the two Russian mathematicians A.S. Merkurjev and A.A. Suslin using algebraic K-theory.

24. $\left(\frac{a,b}{k}\right) \approx \mathcal{M}_2(k)$ if and only if $a = N_{E/k}(z)$ for some $z \in E = k(\sqrt{b})$. Here $N_{E/k}(u + v\sqrt{b}) = u^2 - bv^2$ is the norm, a multiplicative function. [Hint: If $\sqrt{b}$ is in $k$, the result is clear. If not, consider $N(u + i + vj)$ if $u^2 - bv^2 = a$. In the other direction, assume $N(z) = 0$ for some $z \neq 0$ and find the sought-after element by grouping elements appropriately.]

This exercise takes on its true significance when placed in the context number theory, K-theory, and the theory of quadratic forms. We mention three instances:

(i) Look at the first part of J.P. Serre, *A Course in Arithmetic* under "Hilbert symbol". You will find defined there a symbol with the same

formal properties as $\left(\frac{a,b}{k}\right)$ which gives information about quadratic forms. Note that the above problem makes an assertion about when the quadratic form $Q(u,v) = u^2 - bv^2$ assumes the value $a \in k$; namely, it does so when $\left(\frac{a,b}{k}\right) \approx \mathcal{M}_2(k)$. But $\left(\frac{a,b}{k}\right) \approx \mathcal{M}_2(k)$ if and only if $\left(\frac{b,a}{k}\right) \approx \mathcal{M}_2(k)$, by problem 17. This proves the following interesting (and nontrivial) fact : $u^2 - bv^2$ takes the value $a$ if and only if $u^2 - av^2$ takes the value $b$. This is a basic example of what is known as a **reciprocity law** . See Serre's book for other reciprocity laws.

(ii) Look at Samuel, *Algebraic Theory of Numbers* under "quadratic reciprocity"; at least the statement of the theorem. It is a special case of one of the deepest theorems of mathematics. The quadratic case was known to Legendre, but was first proved by Gauss.

(iii) In algebraic K-theory, one defines a functor $K_2$. A theorem of Matsumoto says that for a field $k$, $K_2(k)$ has formal generators $\{a,b\}, a,b \in k^*$ which satisfy the following relations :

(a) Bilinearity: $\{ab,c\} = \{a,c\}\{b,c\}$ and $\{a,bc\} = \{a,b\}\{a,c\}$.

(b) $\{a,b\} = \{b,a\}^{-1}$.

(c) $\{a,1-a\} = 1$ if $a, 1-a \in k^*$.

These relations correspond to properties of generalized quaternion algebras which you (hopefully) proved in the previous few exercises. Thus there is a homomorphism

$$K_2(k)/\{\text{squares}\} \longrightarrow Br(k)$$

given by

$$\{a,b\} \longmapsto \left(\frac{a,b}{k}\right)$$

whose image is the smallest subgroup of $Br(k)$ generated by the quaternion algebras. It was by this method that Merkurjev and Suslin proved that the quaternion algebras generate the part of the Brauer group annihilated by 2 (cf. Exercise 23). For more information about $K_2$, including Matsumoto's Theorem, see J. Milnor, *Introduction to Algebraic K-Theory,* as well as I. Kersten, *Brauergruppen von Körpern.*

25. Show that $\left(\frac{a,b}{k}\right)$ is a division algebra if and only $b$ is not the norm of an element of $k(\sqrt{a})$. [Hint: Use Exercise 24 of Chapter 1.]

26. $\left(\frac{a,b}{k}\right)\otimes_k\left(\frac{a,c}{k}\right)\approx\left(\frac{a,bc}{k}\right)\otimes_k\left(\frac{c,-a^2c}{k}\right)\approx\left(\frac{a,bc}{k}\right)\otimes_k\mathcal{M}_2(k)$. [Hint: Consider the elements $I = i\times 1, J = j\times j', K = IJ, I' = 1\times j', J' = i\times k', K' = I'J'$ and think "double centralizer".]

This exercise gives another formal property of Hilbert symbols; namely, $(a, bc) = (a, b)(a, c)$. When the result is interpreted in $Br(k)$, it says precisely that

$$\left[\left(\frac{a,b}{k}\right)\right]\cdot\left[\left(\frac{a,c}{k}\right)\right]=\left[\left(\frac{a,bc}{k}\right)\right]$$

Together with the fact that $(a, b) = (b, a)$, this shows that the Hilbert symbol is bilinear (or "bimultiplicative", as it is sometimes called due to the multiplicative notation).

27. Prove that an element of $Br(k)$ has the form $[\left(\frac{a,b}{k}\right)]$ for some $a, b \in k$ if and only if it is in $Br(K/k)$ for some separable quadratic extension $K/k$ (remember that an extension $K/k$ is called **quadratic** if it is of degree two).

28. Let $F$ be a field containing a primitive $n$th root of unity $\omega$. For $a, b \in F^*$, let $A_\omega(a, b)$ be the $F$-algebra of dimension $n^2$ which is generated by elements $x$ and $y$ which satisfy $x^n = a, y^n = b$, and $yx = \omega xy$. A basis for $A_\omega(a, b)$ consists of $\{x^iy^j : 0 \le i, j < n\}$. Check the following:

$A_\omega(a, b)$ is central simple over $F$, and thus gives a function

$$a_\omega : F^* \times F^* \longrightarrow Br(F)$$

This function satisfies

$$\begin{aligned}
&a_\omega(a, bc) = a_\omega(a, b)a_\omega(a, c)\\
&a_\omega(a, b) = a_\omega(b, a)^{-1}\\
&a_\omega(a, 1-a) = 1\\
&a_\omega(a, -a) = 1\\
&a_\omega(a, b)^n = 1
\end{aligned}$$

Further, $a_\omega(a, b) = 1$ if and only if $a$ is a norm from $F(\sqrt[n]{b})$. For a local field $F$ with $\omega$ in $F$, there exists $a, b$ such that $a_\omega(a, b)$ has

order exactly $n$. Further information about these algebras and related topics can be found in J.P. Serre, *Local Fields*, J. Milnor, *Introduction to Algebraic K-Theory* (Chapter 15), and L.E. Dickson, *Algebras and Their Arithmetics.*

29. An **involution** of a $k$-algebra $A$ is a $k$-module automorphism $\phi : A \longrightarrow A$ such that $\phi(xy) = \phi(y)\phi(x)$ and $\phi^2(x) = x$ for all $x, y \in A$.

(a) Show that if there is an involution of $A$, then $A^\circ \approx A$.

(b) Find involutions of the $k$-algebras $\mathcal{M}_n(k)$ and $\left(\frac{a,b}{k}\right)$, thus concluding that $\mathcal{M}_n(k) \approx \mathcal{M}_n(k)^\circ$ and $\left(\frac{a,b}{k}\right) \approx \left(\frac{a,b}{k}\right)^\circ$.

(c) Let $A$ be a finite-dimensional central simple $k$-algebra. Prove that if there is an involution $\phi$ of $A$, then $[A]^2 = 1$ in $Br(k)$. Deduce that $[A]^2 = 1$ for every quaternion algebra $A$.

### Another Proof that $Br(K/k) = H^2(Gal(K/k), K^*)$

30. (a) Let $K \supseteq k$ be a finite separable field extension and let $L \supseteq k$ be a splitting field for $K$ relative to $k$ (that is, any irreducible polynomial in $k[x]$ which has a root in $K$ splits completely in $L$). For example, $L$ could be an algebraic closure of $k$, or if $K$ is galois over $k$, then $L$ could be $K$. Let $\sigma_1, \ldots, \sigma_n$ be the distinct $k$-algebra maps from $K$ to $L$, and let $\sigma : K \longrightarrow L^n$ be the maps with components $\sigma_1, \ldots, \sigma_n$. Let $\sigma_L : K_L \longrightarrow L^n$ be the unique $L$-algebra map extending $\sigma$:

$$\sigma_L(a \otimes x) = a \otimes \sigma(x) \qquad \text{for } a \in L, x \in K.$$

Prove that $\sigma_L$ is an isomorphism. Thus the $k$-algebra $K$ "splits completely" when the scalars are extended to $L$.

(b) Let $K$ and $L$ be as in (a). Show that if $D$ is a central simple $k$-algebra with maximal subfield $K$, then $L$ splits $D$. [Hint: Use Exercise 22 to count idempotents.]

(c) If $L$ splits $D$, and if $K$ is a maximal separable subfield of $D$, does $L$ split $K$ relative to $k$ (as in part (a))?

**Remark:** Note that if $K$ is galois over $k$, then we could take $L = K$, obtaining an isomorphism

$$K \otimes_k K \xrightarrow{\approx} \prod_{\sigma \in Gal(K/k)} K.$$

Now suppose that $k$ and $K$ are just commutative rings, not necessarily fields, and that $G$ is a finite group of automorphisms of $K$ with fixed

point set $K^G = k$. We have the obvious map $K \otimes_k K \longrightarrow \prod_{\sigma \in G} K$ described above, and we could define $K/k$ to be a **galois extension of rings** if this map is an isomorphism. Chase, Harrison, and Rosenberg adopt this viewpoint in their paper *Galois Theory and Cohomology of Commutative Rings.* One can also form the crossed product algebra $(K, G, 1)$ arising from the trivial 2-cocycle. They showed that the following are equivalent:

(a) $S \supseteq R$ is a galois ring extension.

(b) $S$ is a finitely generated projective $R$-module, and $(K, G, 1) \approx End_R(S)$.

(c) For every maximal ideal $I \subseteq S$, $G$ acts faithfully on $S/I$.

(d) $S$ is projective as an $S \otimes S^{\circ}$-module, and for every nontrivial idempotent $e \in S$ and $\sigma \neq \tau$ in $G$, there exists $x \in S$ with $\sigma(x)e \neq \tau(x)e$.

This Galois theory of rings is well-developed and useful. The article by Chase, Harrison, and Rosenberg is quite readable and is strongly recommended; see also DeMeyer and Ingraham, *Separable Algebras Over Commutative Rings.*

31. (See, e.g., Herstein, *Noncommutative Rings*) Let $K/k$ be a galois extension with galois group $G$. The fact that $Br(K/k) \approx H^2(G, K^*)$ boils down to the fact that for factor sets $a$ and $b$, $[(K, G, a)][(K, G, b)] = [(K, G, ab)]$. The proof (of Chase) given in the text exhibits a "magic module" on which both $(K, G, a) \otimes_k (K, G, b)$ and $(K, G, ab)$ act. A more direct approach is to choose bases for the first two algebras which give the cocycles $a$ and $b$, respectively, and then try to find a corresponding basis for their tensor product. Their tensor product is not, unfortunately, $(K, G, ab)$, but rather, is matrices over this ring. Hence we must find an appropriate subring of the matrix ring $\mathcal{M}_n((K, G, ab)) \approx (K, G, ab) \otimes_k \mathcal{M}_n(k)$ which is isomorphic to $(K, G, ab)$. This is where Exercise 30 comes in: we now want to list explicitly the idempotents (and their properties) from that exercise. Complete the following outline, which gives the "classical" proof that $Br(K/k) = H^2(G, K^*)$:

(a) Prove that if $A$ is a central simple algebra over $k$ and if $e \neq 0$ is an idempotent element in $A$, then $[A] = [eAe]$ in $Br(k)$. [Hint: Think of $A$ as matrices via the Structure Theorem for Simple Artinian Rings. What does the matrix representing an idempotent element look like?]

(b) Prove that

$$K \otimes_k K = \bigoplus_{\sigma \in G} e_\sigma (K \otimes_k 1) = \bigoplus_{\sigma \in G} e_\sigma (1 \otimes_k K)$$

where $e_\sigma$ are orthogonal idempotents such that $e_\sigma(z \otimes 1) = e_\sigma(1 \otimes \sigma(z))$ for all $z \in K$. Proceed as follows: Since $K/k$ is separable, $K = k(a)$ for some $a \in K$. Let $p(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0$ be the minimal polynomial of $a$ over $k$. Show that $K \otimes_k K$ is a product of copies of $K$ by writing $K = k[x]/(p(x))$. For $\sigma \in G$, let

$$b_{\sigma,m} = a^m \otimes 1 + a^{m-1} \otimes \sigma(a) + \cdots + 1 \otimes \sigma(a)^m.$$

From the fact that $\{1, \sigma(a), \ldots, \sigma(a)^{m-1}\}$ is linearly independent over $k$ for each fixed $\sigma$, deduce that $\{b_{\sigma,1}, \ldots, b_{\sigma,n-1}\}$ is independent over $k$ in $K \otimes_k K$. Now note that

$$(a \otimes 1 - 1 \otimes \sigma(a))b_{\sigma,m} = a^{m+1} \otimes 1 - 1 \otimes \sigma(a)^{m+1}.$$

Deduce that

$$(a \otimes 1 - 1 \otimes \sigma(a))[b_{\sigma,n-1} + \alpha_{n-1}b_{\sigma,n-2} + \cdots + \alpha_1 b_{\sigma,0}] = 0.$$

Hence $a \otimes 1 - 1 \otimes \sigma(a)$ is a (nonzero) zero divisor in $K \otimes_k K$, so there is a minimal idempotent $e_\sigma$ such that $e_\sigma(a \otimes 1 - 1 \otimes \sigma(a)) = 0$ (an idempotent $e$ is a **minimal idempotent** if, whenever $e = e_1 + e_2$ for some commuting idempotents $e_1, e_2$, then $e = e_1$ or $e = e_2$). Show that $e_\sigma(z \otimes 1) = e_\sigma(1 \otimes \sigma(z))$ for all $z \in K$. By comparing dimensions and observing that $e_\sigma \neq e_\tau$ if $\sigma \neq \tau$, show that $e_\sigma e_\tau = 0$ if $\sigma \neq \tau$, and further that

$$\sum_{\sigma \in G} e_\sigma(K \otimes_k K) = \sum_{\sigma \in G} e_\sigma(1 \otimes_k K) = K \otimes_k K.$$

(c) Use parts (a) and (b) to prove that, for factor sets $a$ and $b$,

$$(K, G, a) \otimes_k (K, G, b) \approx (K, G, ab) \otimes_k \mathcal{M}_n(k).$$

Proceed as follows: Let $R = (K, G, a) \otimes_k (K, G, b)$. Since $R \supseteq K \otimes_k K$, part (b) gives $e_\sigma$ as above. Let $e = e_1$. Choose bases $\{x_\sigma\}, \{y_\tau\}$ for $(K, G, a)$ and $(K, G, b)$ which give the cocycles $a$ and $b$, respectively. Show that

$$(1 \otimes y_\tau)e(1 \otimes y_\tau^{-1}) = e_\tau$$
$$(x_\sigma^{-1} \otimes 1)e(x_\sigma \otimes 1) = e_\sigma$$

for all $\sigma, \tau \in G$. Let $w_\sigma = x_\sigma \otimes y_\sigma$. Show that $w_\sigma e = e w_\sigma$. Let $u_\sigma = e w_\sigma$; so $u_\sigma \in eRe$ is invertible in $eRe$ with inverse $e w_\sigma^{-1}$. Show that $u_\sigma u_\tau = u_{\sigma\tau} e(a_{\sigma,\tau} b_{\sigma,\tau} \otimes 1)$. Using the fact that $K \otimes_k K$ is commutative

(so $e(K \otimes_k 1) = (K \otimes_k 1)e$), show that $u_\sigma^{-1} e(x \otimes 1) u_\sigma = e(\sigma(x) \otimes 1$ for $x \in K$. Conclude that $eRe \supseteq (e(K \otimes_k 1), G, e(a \otimes 1)(b \otimes 1))$. By a similar computation, show that $eRe \subseteq \sum u_\sigma e(K \otimes_k 1) \subseteq eRe$, and so $eRe = \sum u_\sigma e(K \otimes_k 1) = (e(K \otimes_k 1), G, e(ab \otimes 1))$. By part (a), $[R] = [eRe]$, so we finally have $[R] = [eRe] = [(K, G, ab)]$ and we are done!

## Norms and Traces

Let $R$ be a finite-dimensional algebra over a field $k$. If $x \in R$, then left multiplication by $x$ is a $k$-endomorphism of $R$. The norm of this $k$-endomorphism is called the **norm** of $x$, denoted $N_{R/k}(x)$; the trace of this $k$-endomorphism is called the **trace** of $x$, denoted $T_{R/k}(x)$. As an example, if $E = k(\sqrt{b})$, the element $u + v\sqrt{b}$ of $E$ gives the matrix $\begin{bmatrix} u & vb \\ v & u \end{bmatrix}$ in the basis $\{1, \sqrt{b}\}$. Thus

$$N_{E/k}(u + v\sqrt{b}) = u^2 - bv^2$$

$$T_{E/k}(u + v\sqrt{b}) = 2u.$$

The definition of norm just given extends that of the norm for generalized quaternion algebras (cf. exercise 21).

32. As above, let $R$ be a finite-dimensional algebra over a field $k$, and let $x \in R$. Show that the following properties hold:

    (a) $N(x) \neq 0$ if and only if $x$ is invertible.

    (b) $N : R^* \longrightarrow k^*$ is a homomorphism.

    (c) $N(a) = a^n$ if $a \in k$, where $n = [R : k]$.

    (d) $T : R \longrightarrow k$ is $k$-linear.

    (e) $T(xy) = T(yx)$.

    (f) $T(a) = na$ for $a \in k$.

33. Prove the following:

    (a) Norm and trace are invariant under extension of scalars. That is, if $S = R_K$ for a field $K$ containing $k$, then

    $$N_{S/K}(x) = N_{R/k}(x) \qquad \text{for } x \in R$$

    and

$$T_{S/K}(x) = T_{R/K}(x) \qquad \text{for } x \in R.$$

(b) Norm and trace are compatible with direct products. That is, if $R = R_1 \times R_2$, then

$$N_{R/k}((x_1, x_2)) = N_{R_1/k}(x_1) \cdot N_{R_2/k}(x_2)$$

and

$$T_{R/k}((x_1, x_2)) = T_{R_1/k}(x_1) + T_{R_2/k}(x_2).$$

(c) If $x \in J(R)$ then $N(1+x) = 1$ and $T(x) = 0$.

(d) In the notation of Exercise 30,

$$N_{K/k}(x) = \prod_i \sigma_i(x)$$

and

$$T_{K/k}(x) = \sum_i \sigma_i(x).$$

(e) If $R = \mathcal{M}_n(k)$, then

$$N_{R/k}(x) = (det(x))^n$$

and

$$T_{R/k}(x) = n \cdot trace(x).$$

This suggests the definition of more useful functions, called the **reduced trace** and **reduced norm** ; Reiner, *Maximal Orders*, or Bass, *Algebraic K-Theory* for details.

34. A **bilinear form** $B(x, y)$ on a finite-dimensional vector space $V$ over a field $k$ is a function $B : V \times V \longrightarrow k$ which is linear as a function of one variable when the other is kept fixed. $B$ is said to be **non-degenerate** if the following equivalent criteria hold:

(a) If $x \in V$ satisfies $B(x, y) = 0$ for all $y \in V$, then $x = 0$.

(b) The map $f : V \longrightarrow V^* = Hom_k(V, k)$ defined by $f(x)(y) = B(x, y)$ is an isomorphism.

(c) For any basis $e_1, \ldots, e_n$ of $V$ the matrix $(B(e_i, e_j))$ is invertible.

(d) For some basis, the matrix $(B(e_i, e_j))$ is invertible.

Show that these four conditions are equivalent. Recall that a finite-dimensional algebra $R$ over $k$ is called separable over $k$ if its center is a product of separable field extensions of $k$. Prove that if $char(k) = 0$ or if $R$ is commutative, then $R$ is separable if and only if the bilinear form $B(x,y) = T_{R/k}(xy)$ is non-degenerate. [Hint: Use the fact that the trace is invariant under extension of scalars.]

**Remark:** This is no longer true if $k$ has non-zero characteristic and $R$ is noncommutative. If $R = \mathcal{M}_n(k)$ and $char(k) = p$, $p$ a prime dividing $n$, then $T_{R/k} = 0$.

35. Let $K$ be a galois extension of $k$ with Galois group $G$ which is cyclic of order $n$. Prove that $Br(K/k) \approx k^*/N_{K/k}(K^*)$. [Hint: It is possible to deduce this from the isomorphism of $Br(K/k)$ with $H^2(G, K^*)$, but it is easier to go back to the proof of this isomorphism and observe that the situation is much simpler when $G$ is cyclic. Let $x_\sigma$ be chosen for $\sigma$ a generator of $G$. Use this element to choose all the other basis elements in an obvious way.]

36. Use the preceding problem to give another proof of the Frobenius Theorem that the only finite-dimensional central division algebras over $\mathbf{R}$ are $\mathbf{R}$ and $\mathbf{H}$. Also give another proof of Wedderburn's Theorem that all finite division rings are commutative. Do these by computing the respective Brauer groups. It is yet another indication of the power of the Brauer theory that it subsumes these two celebrated results.

### Cohomology and Applications

37. Prove Proposition 4.11 : $\delta^2 = 0$.

38. Let $G$ be a finite group and let $M$ be a $G$-module. Show by a direct argument that every element of $H^n(G, M)$ is annihilated by $|G|$ for $n > 1$.

**Remark:** There is a more conceptual way to do this: for a subgroup $H \subseteq G$, there are useful maps (which we will discuss in the exercises later in this chapter) $Res : H^n(G, M) \longrightarrow H^n(H, M)$ and $Cor : H^n(H, M) \longrightarrow H^n(G, M)$ (the classical "transfer maps" of group theory) such that $Cor \circ Res : H^n(G, M) \longrightarrow H^n(G, M)$ is just

multiplication by $[G : H]$. In particular, taking $H = 1$, the trivial group, we see that multiplication by $|G|$ is just the composite

$$H^n(G, M) \xrightarrow{Res} H^n(1, M) \xrightarrow{Cor} H^n(G, M)$$

But $H^n(1, M) = 0$, so this composite is the zero map, and so $|G|$ annihilates $H^n(G, M)$. For more details on this, see K. Brown, *Cohomology of Groups.*

39. Try to understand the following argument, checking statements and filling in details as needed: By Theorem 4.13, $H^2(G, K^*) \approx Br(K/k)$ and hence classifies central simple algebras. By an entirely similar argument, one can show that, for a $G$-module $M$, $H^2(G, M)$ classifies extensions

$$1 \longrightarrow M \longrightarrow E \longrightarrow G \longrightarrow 1$$

inducing the given $G$-action on $M$ (see K. Brown, *Cohomology of Groups*). If $M$ is finite and $|M|$ is prime to $|G|$, then note that:

(a) Multiplication by $|G|$ is an automorphism of $M$, and so induces an automorphism of $H^2(G, M)$.

(b) Multiplication by $|G|$ kills $H^2(G, M)$ by the above problem. Thus the only possibility is that $H^2(G, M) = 0$; that is, there is only one extension $1 \longrightarrow M \longrightarrow E \longrightarrow G \longrightarrow 1$, the split one. Put another way : If $E$ is a group and $M$ is an abelian normal subgroup such that $G = E/M$ has order prime to $|M|$, then $E$ is a semidirect product $E = M \rtimes G$. Finally, by suitable cleverness, one can reduce the arbitrary case ($M$ non-abelian) to the case of $M$ abelian, thus giving the following

**Theorem 4.20 (Schur-Zassenhaus)** *If $G$ is a finite group, $H \lhd G$ a normal subgroup with $|H|$ prime to $[G : H]$, then $G$ is a semidirect product $G = H \rtimes (G/H)$.*

40. Prove the following corollary to the above discussion :

**Corollary 4.21** *Let $A$ be a finite-dimensional central simple $k$-algebra with galois splitting field $L$, and let $n = [L : k]$. Then*

$$\underbrace{A \otimes_k A \otimes_k \cdots \otimes_k A}_{n} \approx \mathcal{M}_m(k)$$

*for some $m$.*

Reflect upon how hard this would be to prove without use of cohomology.

41. Prove Hilbert's so-called 'Theorem 90' : If $K/k$ is a galois extension and $G = Gal(K/k)$, then $H^0(G, K^*) = k^*$ and $H^1(G, K^*) = 1$. [Hint : Let $f : G \longrightarrow K^*$ satisfy $(\delta_1(f)(\sigma, \tau) = 1$ for all $\sigma, \tau \in G$. Now show that there exists $a \in K^*$ such that $b = \sum_{\sigma \in G} f(\sigma)\sigma(a) \neq 0$. Deduce that $\tau(b) = f(\tau)^{-1}b$ for all $\tau \in G$, so that $f \in B^1(G, K^*)$.]

42. (a) Let $G$ be a group and let $H$ be a subgroup. Let $M$ be a $G$-module. Show that by restricting a function from $G \times \cdots \times G \longrightarrow M$ to a function $H \times \cdots \times H \longrightarrow M$ we obtain a homomorphism of cochain groups

$$Res^G_H : C^n(G, M) \longrightarrow C^n(H, M).$$

"*Res*" stands for "restriction". The map is called this for obvious reasons. Show that $Res^G_H$ maps $Z^n(G, M)$ into $Z^n(H, M)$ and $B^n(G, M)$ into $B^n(H, M)$, and hence induces a homomorphism

$$Res^G_H : H^n(G, M) \longrightarrow H^n(H, M).$$

(b) Let $k \subseteq F \subseteq K$ be fields. Show that extension of scalars induces a map

$$Res^F_k : Br(K/k) \longrightarrow Br(K/F)$$

given by $Res^F_k([A]) = [F \otimes_k A]$.

(c) Let $K/k$ be a galois extension with Galois group $G$. Let $H$ be a subgroup of $G$ and let $F$ be the corresponding fixed field. Let $f$ be a factor set satisfying the cocycle condition. Let $A = (K, G, f)$ be the central simple $k$-algebra constructed in the proof of the isomorphism of the Brauer group with $H^2(G, K^*)$. Let $\{x_\sigma : \sigma \in G\}$ be the usual $K$-basis of $A$, that is, $x_\sigma u = \sigma(u)x_\sigma$ and $x_\sigma x_\tau = f_{\sigma,\tau}x_{\sigma\tau}$. Prove that $\{x_\sigma : \sigma \in H\}$ is a $K$-basis $C(F)$.

(d) Let $k \subseteq F \subseteq K$ and $H$ a subgroup of $G$ as in part (c). Show that the following diagram commutes:

$$\begin{array}{ccc} H^2(G,K^*) & \longrightarrow & Br(K/k) \\ \Big\downarrow {\scriptstyle Res^G_H} & & \Big\downarrow {\scriptstyle Res^F_k} \\ H^2(H,K^*) & \xrightarrow{\approx} & Br(K/F) \end{array}$$

43. (a) Let $G$ be a group, $H$ a normal subgroup, and $M$ a $G$-module. Show that $M^H = \{m \in M : \sigma(m) = m \quad \text{for all } \sigma \in H\}$ is a $G/H$-module. Show that there is a homomorphism

$$Inf_H^G : H^2(G/H, M^H) \longrightarrow H^2(G, M)$$

which sends a cocycle $f$ to the function defined by $(\sigma, \tau) \longmapsto f(\sigma H, \tau H)$. "$Inf$" stands for "inflation" because it gives a map from the cohomology of a quotient group $G/H$ into the cohomology of the (inflated) full group $G$.

(b) Let $k \subseteq F \subseteq K$ be fields such that $[K : k] < \infty$. Let $B$ be a central simple $k$-algebra with maximal commutative subring $F$. Considering $K \otimes_F B$ as a right $B$-module, show that $A = End_B(K \otimes_F B)$ is a central simple $k$-algebra with maximal commutative subring $F_K$. Further, show that $[A] = [B]$ in $Br(k)$.

(c) Let $k \subseteq F \subseteq K$ be as in part (b). Assume further that $K$ is galois over $k$ with Galois group $G$, and that $F$ is the fixed subfield of the normal subgroup $H$. Show that the following diagram commutes:

$$\begin{array}{ccc} H^2(G/H, F^*) & \xrightarrow{\approx} & Br(F/k) \\ \Big\downarrow {\scriptstyle Inf_H^G} & & \Big\downarrow \\ H^2(G, K^*) & \xrightarrow{\approx} & Br(K/k) \end{array}$$

44. Let $k \subseteq F \subseteq K$ be fields with $E/K$ and $K/k$ galois extensions. Show that the sequence

$$0 \longrightarrow H^2(Gal(F/k), F^*) \xrightarrow{Inf} H^2(Gal(K/k), K^*)$$
$$\xrightarrow{Res} H^2(Gal(K/F), K^*) \longrightarrow 0$$

is exact.

# Part II

# Selected Topics

# 5

# Primitive Rings and the Density Theorem

We saw in Theorem 1.15 that simple artinian rings are precisely those artinian rings which have a faithful simple module. It is useful to drop the finiteness condition and to study those rings which have a faithful simple module but are not necessarily artinian. Such a ring is called a **primitive ring**. Primitive rings, a generalization of simple rings, play a role analogous to that of simple rings in that they may be viewed as the basic building blocks of other rings, though in an extended, infinite dimensional context. This perhaps justifies the name primitive. The theory of primitive rings can be developed along lines parallel to that of simple rings. The two theories intertwine, and in fact some authors choose to study simple rings from the point of view of primitive rings. This chapter explores such an approach.

**Definition:** A ring $R$ is called **primitive** if it has a faithful simple module.

It should be noted that some of the terms in this definition are often given other names. Recall that giving an $R$-module $M$ is the same as giving a homomorphism $\rho$ of $R$ into $End(M)$, the ring of abelian group homomorphisms of $M$. $\rho$ is often called a **representation** of $R$ (acting on $M$). An **irreducible representation** of $R$ is a representation for which the associated module is irreducible (i.e., simple). Thus a primitive ring is one which has a faithful irreducible representation. We will pick up this terminology in a later chapter on representation theory.

**Examples:**

1. Any simple ring is primitive; in particular, any finite dimensional matrix ring over a division ring is primitive. This follows from the fact that any nonzero ring $R$ has a maximal left ideal $I$, and if $R$ is simple then $I$ contains no nonzero ideal, so $R/I$ is a faithful simple module for $R$. It should be noted that the zero ring is simple but not primitive, but in this book we are only considering rings with identity 1, with $1 \neq 0$, so the zero ring doesn't count.

2. Let $V$ be a vector space, not necessarily finite dimensional, over a division ring $D$. Then $R = End_D(V)$ has $V$ as a faithful simple

module and is thus primitive. Clearly $V$ is a faithful $R$-module. To show that $V$ is a simple $R$-module, we need to see that for any $v, w \in V$, there is a $\phi \in R$ with $\phi(v) = w$, but this is clear since $v$ is part of a basis for $V$. As noted in exercise 28 of Chapter 1, $R$ is not simple if $V$ is not finite dimensional over $D$. This gives an example of a ring which is primitive but not simple.

Other examples of primitive rings can be found in the exercises at the end of this chapter and in Part III.

There is another, more ring-theoretic approach to proving the Structure Theorem for Simple Artinian Rings than was taken in Chapter 1. This alternate line of attack uses the Jacobson Density Theorem, a theorem which has applications throughout ring theory. We first begin with a

**Definition:** Let $V$ be a vector space over a division ring $D$, and let $R$ be a ring of $D$-linear transformations of $V$. $R$ is called a **dense** ring of linear transformations, or is said to **act densely** on $V$, if for every finite set $\{v_1, \ldots, v_n\}$ of linearly independent vectors in $V$, and any set $\{w_1, \ldots, w_n\}$ of (not necessarily independent) vectors in $V$, there exists a linear transformation $\phi \in R$ with

$$\phi(v_i) = w_i \quad \text{for } i = 1, \ldots, n.$$

Let $R$ be a dense ring of linear transformations of a finite dimensional vector space over a division ring $D$ with basis $\{v_1, \ldots, v_n\}$. For any $\psi \in End_D(V)$, there must be $\phi \in R$ with $\phi(v_i) = \psi(v_i)$, since $R$ is dense. But $\{v_1, \ldots, v_n\}$ is a basis for $V$, so $\psi = \phi \in R$. Thus the only dense ring of linear transformations of $V$ is the ring $End_D(V)$.

For those who wonder where the topological term "dense" comes from in the above definition, let $V$ be given the discrete topology, and let $End_D(V)$ be given the compact-open topology as a space of functions on the space $V$. Then it is not hard to check that a ring $R$ of linear transformations acts densely on $V$ if and only if $R$ is dense as a subspace of $End_D(V)$.

Before proving the main theorem of this chapter, the Jacobson Density Theorem, we prove a similar theorem in the context of semisimple modules which will be used to prove Jacobson's Theorem.

**Theorem 5.1 (Density Theorem For Semisimple Modules)** *Let $M$ be a semisimple module over a ring $R$, and let $S = End_R(M)$. Let $\phi \in End_S(M)$. Then for any set $\{x_1, \ldots, x_n\}$ of $M$, there exists $r \in R$ such that*

$$\phi(x_i) = rx_i \quad \textit{for } i = 1, \ldots, n.$$

*Thus the action of any $S$-module endomorphism of $M$ on a finite set can be achieved by the action of an element of $R$.*

Note that $\{x_1, \ldots, x_n\}$ in the hypothesis of the theorem is not assumed to be a linearly independent set.

**Proof:** We first prove the theorem in the case $n = 1$. Let $x_1$ be given. Since $M$ is semisimple we can write

$$M = Rx_1 \oplus M'$$

for some submodule $M'$ (every submodule is a direct summand). If $\pi : M \longrightarrow Rx_1$ is the projection map, then $\pi \in S$, and so

$$\phi(x_1) = \phi(\pi(x_1)) = \pi(\phi(x_1)).$$

But $\{y \in M : \pi(y) = y\}$ is just $Rx_1$. Thus $\phi(x_1) \in Rx_1$ as desired.

Now suppose we are given the set $\{x_1, \ldots, x_n\}$ of $M$. At first suppose $M$ is simple. Look at the product map $\phi^{(n)} : M^n \longrightarrow M^n$ defined by

$$\phi^{(n)}(y_1, \ldots, y_n) = (\phi(y_1), \ldots, \phi(y_n)).$$

Then $End_R(M^n) = \mathcal{M}_n(S)$ by Proposition 1.7. Now $\phi$ and $S$ both act on $M$, and the actions commute, so $\phi^{(n)} \in End_{End_R(M^n)}(M^n)$, so by the proof of the theorem in the $n = 1$ case there exists $r \in R$ with

$$(rx_1, \ldots, rx_n) = \phi^{(n)}(x_1, \ldots, x_n) = (\phi(x_1), \ldots, \phi(x_n))$$

and the theorem is proved for simple $M$.

If $M$ is semisimple then $M$ is a direct sum of its isotypic constituents

$$M \approx M_1^{n_1} \oplus \cdots \oplus M_r^{n_r} \quad \text{with} \quad M_i \not\approx M_j \text{ if } i \neq j.$$

The matrices representing the endomorphisms break up into blocks, and the reader may check that the same argument as above will work. □

The Density Theorem for Semisimple Modules may be used to prove a density theorem for primitive rings due to Jacobson. This useful result may be viewed as an analog to the Structure Theorem for Simple Artinian Rings.

**Theorem 5.2 (Jacobson Density Theorem)** *A ring $R$ is primitive if and only if it is a dense ring of linear transformations of a vector space over a division ring.*

It is interesting to note that Jacobson, in his book *Basic Algebra II*, calls this theorem the "Density Theorem for Primitive Rings", although it is most commonly known as the Jacobson Density Theorem.

**Proof:** Suppose $R$ is primitive, and that $M$ is a faithful simple $R$-module. Then $D = End_R(M)$ is a division ring by Schur's Lemma. Since $M$ is

faithful, $R$ acts (by left multiplication) as a ring of linear transformations on $M$ considered as a vector space over the division ring $D$. Given a set $\{v_1, \ldots, v_n\}$ of linearly independent (over $D$) vectors in $M$, and any set $\{w_1, \ldots, w_n\}$ of vectors in $M$, we may take (by linear independence) the $v_i$'s as part of a basis for $M$, and so there exists a linear transformation $\phi$ such that

$$\phi(v_i) = w_i \quad i = 1, \ldots, n.$$

But $\phi \in End_D(M)$ and $D = End_R(M)$, so by the Density Theorem for Semisimple Modules there exists $r \in R$ with

$$rx_i = \phi(x_i) = y_i \quad i = 1, \ldots, n.$$

Thus $R$ is a dense ring of endomorphisms of $M$.

Conversely, suppose that $R$ is a dense ring of endomorphisms of a vector space $V$ over a division ring $D$. Then $V$ is an $R$-module via

$$\phi \cdot v = \phi(v) \quad \text{for } \phi \in R, v \in V.$$

$V$ is clearly a faithful $R$-module, and is simple since, given any $v \neq 0$ in $V$, $v$ is part of a basis for $V$, and so for any $w \in V$ there is a linear transformation $\phi \in R$ with $\phi(v) = w$; that is, $w \in Rv$. Thus $R$ is primitive, as it has a faithful simple module. □

The 'if' direction of the Jacobson Density Theorem can be made stronger. A set $R$ of endomorphisms of a vector space $V$ over a division ring $D$ is called **$n$-fold transitive** if, for any $m \leq n$, any set $\{x_1, \ldots, x_m\}$ of $m$ linearly independent vectors in $V$ and any set $\{y_1, \ldots, y_m\}$ of vectors in $V$, there exists $\phi \in R$ with $\phi(x_i) = y_i$ for all $1 \leq i \leq m$. Now if $R$ is a ring of endomorphisms of $V$ over $D$ which is even just 1-fold transitive, then $R$ is primitive. To see this, note that by definition $V$ is a faithful $R$-module, and is simple by transitivity. Thus we have a stronger implication in the 'if' direction of the density theorem, although there is another intricacy involved (see Exercise 9).

One may derive a plethora of results from the Jacobson Density Theorem; we mention but two. Many authors derive the Structure Theorem for Simple Artinian Rings as a consequence of Jacobson's Theorem. We now take this approach.

**Theorem 5.3 (Simple artinian rings revisited)** *Any simple artinian ring is isomorphic to a finite dimensional matrix ring over a division ring.*

We don't bother to derive the corresponding theorem for semisimple rings (Wedderburn's Theorem) and the uniqueness results, for these follow as in Chapter 1.

**Proof:** Let $R$ be a simple artinian ring. $R$ is primitive since $R$ is simple (Example 1 on page 151). Let $M$ be a faithful simple $R$-module, and let $D = End_R(M)$, which is a division ring by Schur's Lemma. By the Jacobson Density Theorem we know that $R$ is isomorphic to a dense subring of $End_D(M)$. If $M$ is finite dimensional over $D$, then as noted previously a dense subring of a finite dimensional endomorphism ring is the whole ring of endomorphisms, so in this case $R = End_D(M)$ and we are done.

So suppose that $v_1, v_2, \ldots$ is an infinite linearly independent set of vectors in the vector space $M$ over $D$. Let $I_n$ be the left ideal of $R$ defined by

$$I_n = \{r \in R : rv_i = 0 \text{ for all } 1 \leq i \leq n\}.$$

Clearly $I_1 \supset I_2 \supset \cdots$ is a descending chain of left ideals. In fact it is a properly descending chain by the Density Theorem for Semisimple Modules, since by the theorem there is an element $r \in R$ with $rv_i = 0$ for $1 \leq i \leq n$, but with $rv_{n+1} \neq 0$. This infinite descending chain contradicts the hypothesis that $R$ is artinian, so $M$ is in fact finite dimensional over $D$ and we are done. □

As another consequence of the Jacobson Density Theorem one may derive a structure theorem for primitive rings which is similar to that for simple artinian rings, although as one might expect considering the finiteness condition is dropped, part of the structure theorem has to deal with the cases when the ring is quite big.

**Theorem 5.4 (Structure Theorem for Primitive Rings)** *Let $R$ be a primitive ring with faithful simple module $M$. Let $D = End_R(M)$ ($D$ is a division ring by Schur's Lemma). Then either $R = \mathcal{M}_n(D)$ for some $n$ or, for every positive integer $m$, there exists a subring $R_m$ of $R$ which maps homomorphically onto $\mathcal{M}_m(D)$.*

**Proof:** The proof is similar to that of Theorem 5.3. As before, if $M$ has finite dimension over $D$ then $R = End_D(M) = \mathcal{M}_n(D)$ for some $n$. If $v_1, v_2, \ldots$ is an infinite linearly independent set of vectors in the vector space $M$ over $D$, then let $M_m$ be the $D$-subspace of $M$ spanned by $\{v_1, \ldots, v_m\}$, let

$$R_m = \{r \in R : rV_m \subseteq V_m\}$$

and, as in the proof of Theorem 5.3, let

$$I_m = \{r \in R : rv_i = 0 \text{ for all } 1 \leq i \leq m\}.$$

Then $I_m$ is an ideal in the subring $R_m$ of $R$, and $R_m/I_m \approx \mathcal{M}_m(D)$ by the Jacobson Density Theorem. This proves the theorem. □

It seems that one could use the Structure Theorem for Primitive Rings to prove Theorem 5.3 (that every simple artinian ring is isomorphic to a matrix ring), for it seems unlikely that a ring with subrings mapping onto arbitrarily large matrix rings could be artinian. Such rings do, however, exist; even division rings with this property exist! See Part III, Exercise 27 for an example. This shows that primitive rings may be quite unweidly; indeed, every algebra is the image of some primitive algebra under some homomorphism (Exercise 15).

As noted in the examples on page 151, every simple ring is primitive but not every primitive ring is simple. The Structure Theorem for Primitive Rings also lends credence to the notion that primitive rings extend the notion of simple ring to the infinite dimensional context. In fact it is not difficult to show that a ring is primitive artinian if and only if it is simple artinian (if and only if it is a finite dimensional matrix ring); thus the concepts of primitive and simple agree in the finite dimensional case. We leave this fact as an exercise to the reader (Exercise 8).

# Exercises

## Primitive Rings

1. Let $V$ be a vector space over a division ring $D$. Let $V$ be given the discrete topology and let $End_D(V)$ be given the compact-open topology as a space of functions on the space $V$. Show that a ring $R$ of linear transformations acts densely on $V$ if and only if $R$ is dense as a subspace of $End_D(M)$.

2. (a) Show that a ring is primitive if and only if it contains a maximal left ideal that contains no nonzero ideal.

   (b) Show that a commutative ring is primitive if and only if it is a field.

3. Show that $\mathcal{M}_n(R)$ is primitive if $R$ is primitive.

4. Let $V$ be a vector space of countably infinite dimension over a division ring $D$, and choose a basis for $V$ over $D$. Let $R$ denote the set of linear transformations represented by matrices of the form

$$\begin{bmatrix} A & & & 0 \\ & d & & \\ & & d & \\ 0 & & & \ddots \end{bmatrix}$$

   where $A$ is a finite square matrix and $d \in D$. Check that $R$ is a subring of the ring of row-finite matrices (matrices with only finitely many nonzero entries in each row). Show that $R$ is primitive.

5. Let $V$ be the vector space $\mathbf{Q}[x]$, $x$ an indeterminate. Let $d$ denote the "differentiation map" defined by

$$d(c_n x^n + \cdots + c_1 x + c_0) = nc_n x^{n-1} + \cdots + c_1$$

and let $i$ denote the "integration map (with constant term 0)" defined by

$$i(c_n x^n + \cdots + c_1 x + c_0) = \frac{c_n}{(n+1)} x^{n+1} + \cdots c_0 x.$$

Check that both $d$ and $i$ are $\mathbf{Q}$-endomorphisms of $V$. Let $R$ be the subalgebra of $End_{\mathbf{Q}}(V)$ generated by $\mathbf{Q}, d$, and $i$. Show that $R$ is primitive.

6. Let $e$ be a nonzero idempotent of the ring $R$. Recall (Chapter 0, Exercise 27) that $eRe$ is a ring with $e$ as identity element. Show that $eRe$ is primitive if $R$ is primitive.

7. In the proof of the Structure Theorem for Primitive Rings, show that $R$ is artinian if and only if the faithful simple $R$-module $M$ has finite dimension over the division ring $D = End_R(M)$.

8. Show that a ring is primitive artinian if and only if it is simple artinian. [Hint: Look at the proof of the Structure Theorem for Primitive Rings.]

### More on the Converse to the Density Theorem

9. (a) We showed above that if $R$ is a 1-fold transitive ring of endomorphisms of a vector space $V$ over a division ring $D$, then $R$ is primitive. Show that in this case, however, the commuting ring of $R$ need not equal $D$ (recall that the **commuting ring** of $R$ is the set of endomorphisms in $End_R(M)$ which commute with all of the endomorphisms $\phi_r$ given by scalar multiplication with $r \in R$).

   (b) Now assume that $V$ is finite dimensional. Characterize all simple subrings of $\mathcal{M}_n(D)$ (see Chapter 3, Exercise 34).

   (c) Still assuming $V$ is finite dimensional, characterize all primitive subrings of $\mathcal{M}_n(D)$.

10. Show that any ring $R$ of 2-fold transitive endomorphisms of a vector space $V$ over a division ring $D$ is dense, and so is n-fold transitive for all $n$. Thus in this case the commuting ring of $R$ is precisely $D$. [Hint: Show first that, if $v \in V$ and $\phi \in End_R(V)$, then $v$ and $\phi(v)$ are linearly independent over $D$, as long as $dim_D(V) \geq 2$.]

## Semi-Primitive Rings

A ring $R$ is called **semi-primitive** if for any element $a \neq 0$ of $R$, there is a simple $R$-module $M$ with $a \notin ann(M)$. The relationship between semi-primitive rings and semisimple rings is reminiscent of that between primitive rings and simple rings. In studying semi-primitive rings it will be useful to generalize the concept of direct product. If $\{R_\alpha\}$ is any family of rings, and if $\pi_\beta : \prod R_\alpha \longrightarrow R_\beta$ is the natural projection, then $R$ is said to be a **subdirect product** of the rings $R_\alpha$ if there is a monomorphism $i : R \longrightarrow \prod R_\alpha$ such that $\pi_\beta \circ i : R \longrightarrow R_\beta$ is surjective for each $\beta$.

11. Show that the following three conditions on a ring $R$ are equivalent:

    (i) $R$ is semi-primitive.

    (ii) $R$ has a faithful semisimple module.

    (iii) $R$ is a subdirect product of primitive rings.

12. (a) Show that a commutative ring is semi-primitive if and only if it is a subdirect product of fields.

    (b) Show that $\mathbf{Z}$ is semi-primitive, as is any principal ideal domain with an infinite number of primes.

13. (a) Show that a ring $R$ is semi-primitive if and only if $J(R) = 0$, where $J(R)$ denotes the (Jacobson) radical of $R$.

    (b) Show that $R/J(R)$ is semi-primitive, and that $J(R)$ is the intersection of all ideals $I$ of $R$ such that $R/I$ is primitive.

14. Show that $R$ is semisimple artinian if and only if $R$ is semi-primitive artinian.

## Applications of the Density Theorem

15. Let $A$ be an algebra over the field $k$, and let $V$ be a direct sum of infinitely many copies of $A$. Consider the subring $R$ of $End_k(V)$ generated by $A$ (acting diagonally) and the set of linear transformations which are nonzero on at most finitely many terms of the direct sum (these transformations are sometimes said to have **finite support**). Show that $R$ is primitive and that there is a surjection of $R$ onto $A$. Thus any $k$-algebra is the image of some primitive $k$-algebra under some homomorphism.

16. The goal of this exercise is to prove a very nice theorem of Jacobson that gives a condition on the powers of elements of a ring that will make the ring commutative. The condition is that for every element $r$ of the ring, there is some integer $n(r) > 1$ so that $r^{n(r)} = r$. It

seems quite strange that a ring with such a property must necessarily be commutative, and even strange that any condition of this nature should imply commutativity. This theorem can be proved using techniques from this chapter.

(a) Show that if $R$ is a primitive ring with the property that, for each $r \in R$, there is an integer $n(r) > 1$ such that $r^{n(r)} = r$, then $R$ is a division ring.

(b) Show that the ring in part (a) is in fact a field. [Hint: Show that $R$ has finite characteristic $p$. If $R = Z(R)$ we are done, otherwise choose $r \in R, r \notin Z(R)$. Use the generalized Skolem-Noether Theorem (Chapter 3, Exercise 18) to find an $s \in R$ with $srs^{-1} = r^p$. Show that $r$ and $s$ generate a finite division ring.]

(c) Let $R$ be any ring such that, for any $r \in R$, there is an integer $n(r) > 1$ such that $r^{n(r)} = r$. Show that $R$ is semi-primitive.

(d) Prove the following theorem of Jacobson: If $R$ is any ring such that, for any $r \in R$, there is an integer $n(r) > 1$ such that $r^{n(r)} = r$, then $R$ is commutative.

**Remark:** The theorem you just proved has vast generalizations, and indeed there is a whole theory of commutativity of which this is one of the foundling steps. For an introduction to commutativity theorems see Herstein, *Noncommutative Rings.*

# 6

# Burnside's Theorem and Representations of Finite Groups

In this chapter we provide an application of the structure theory of rings developed in Chapters One and Two to the theory of finite groups. Representation theory of finite groups is a vast subject; in this chapter we'll make a thin beeline right to a famous theorem of Burnside. For a more thorough introduction to the representation theory of finite groups, the reader may consult Serre, *Linear Representations of Finite Groups*, as well as Fulton and Harris, *Representation Theory : A First Course.*

Unless otherwise specified, $G$ will denote a finite group throughout this chapter. We will only discuss representation over the field $\mathbf{C}$ of complex numbers, as this suffices for the desired applications.

## Group Representations

We begin with a rephrasing of some of the ring theory we have learned into the language of representation theory.

**Definition:** A **representation** of a group $G$ is a homomorphism $\rho : G \longrightarrow GL(V)$ , where $GL(V)$ is the algebra of automorphisms of a vector space $V$ over a field $k$. The dimension of $V$ over $k$ (which we will assume to be finite throughout this chapter) is called the **degree** of the representation.

**Note:** Henceforth we will assume that $k = \mathbf{C}$, and by "representation" we will mean a representation over the complex numbers, which is usually called a **complex representation**. Although representations over other fields, in particular fields of nonzero characteristic, are extremely important, restricting our attention to representations over $\mathbf{C}$ will simplify matters greatly, and suffices for the applications we wish to give. When working with complex representations, the two most important properties of the field $\mathbf{C}$ which will be used are the facts that the order of the group $G$ is invertible in the field $\mathbf{C}$, and $\mathbf{C}$ is algebraically closed.

If $V$ is $n$-dimensional and if we pick a basis $\mathcal{B}$ for $V$ over $\mathbf{C}$, then $GL(V)$ can be thought of as the group of $n \times n$ invertible matrices over $\mathbf{C}$, denoted $GL_n(\mathbf{C})$. In this way the representation $\rho$ assigns a matrix $\rho_{\mathcal{B}}(g)$ to each group element $g$, and we call $\rho$ a **matrix representation** of $G$ (sometimes we refer to a matrix representation without explicitly choosing a basis). If $\mathcal{A}$ and $\mathcal{B}$ are bases for $V$ over $\mathbf{C}$, and if $C$ is the change of basis matrix from $\mathcal{A}$ to $\mathcal{B}$, then the matrices $\rho_{\mathcal{A}}(g)$ and $\rho_{\mathcal{B}}(g)$ are related by : $\rho_{\mathcal{B}}(g) = C^{-1}\rho_{\mathcal{A}}(g)C$. If $\rho$ is a matrix representation, we denote the $(i, j)$-entry of the matrix $\rho(\sigma)$ by $\rho_{ij}(\sigma)$ for $\sigma \in G$.

Notice that $V$ is a module over the group ring $\mathbf{C}[G]$, where the action of the ring is defined by $g{\cdot}v = \rho(g)(v)$ for $g \in G, v \in V$ and is extended linearly to $\mathbf{C}[G]$. Conversely, a $\mathbf{C}[G]$-module $V$ gives a representation $\rho : G \longrightarrow GL(V)$ defined by $\rho(g)(v) = g \cdot v$, where $g \cdot v$ denotes the multiplication of a module element by a scalar. Hence the study of representations of $G$ is equivalent to the study of $\mathbf{C}[G]$-modules.

Two representations $\rho : G \longrightarrow GL(V)$ and $\rho' : G \longrightarrow GL(V')$ are **equivalent** if $V$ and $V'$ are isomorphic as $\mathbf{C}[G]$-modules. Note that this is the same as saying that $\rho'(g) = T\rho(g)T^{-1}$ for all $g \in G$, where $T : V \longrightarrow V'$ is a $\mathbf{C}$-module isomorphism.

**Examples:**

1. Letting $V$ be one-dimensional and letting $\rho : G \longrightarrow GL(V)$ be $\rho(g) = 1$ for all $g \in G$, where '1' here denotes the identity element of $GL(V)$, gives a representation called the **trivial representation** of $G$.

2. A degree one representation is simply a homomorphism $\rho : G \longrightarrow \mathbf{C}^*$. Note that since $G$ has finite order each $\rho(g)$ is a root of unity; in particular $|\rho(g)| = 1$ for all $g \in G$. When $G = \mathbf{Z}/n\mathbf{Z}$, the cyclic group of order $n$, then it is clear that each $n$th root of unity gives a degree one representation over $\mathbf{C}$, so that there are precisely $n$ representations of $\mathbf{Z}/n\mathbf{Z}$ of degree one over $\mathbf{C}$.

3. The group algebra $\mathbf{C}[G]$ is a left module over itself, which gives a representation of $G$. This most fundamental and important representation is called the **(left) regular representation** of $G$; it is a degree $|G|$ representation. Note that $g \in G$ acts by left multiplication on elements of $\mathbf{C}[G]$, giving an element of $End_{\mathbf{C}}(\mathbf{C}[G])$. For example, let $G = \{1, x, x^2, x^3\}$ be the cyclic group of order 4. The group element $x^2 \in G$ acts on the standard $\mathbf{C}$-basis $\{1, x, x^2, x^3\}$ of the group ring $\mathbf{C}[G]$ by multiplication on the left :

$$x^2 \cdot 1 = x^2, \quad x^2 \cdot x = x^3, \quad x^2 \cdot x^2 = 1, \quad x^2 \cdot x^3 = x.$$

   Thus if $\rho$ is the regular representation of $G$, we have

$$\rho(x^2) = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

**Definition:** A simple $\mathbf{C}[G]$-module $V$ (and the associated representation $\rho : G \longrightarrow GL(V)$) is called an **irreducible representation**.

Notice from the Wedderburn Theory (cf. the discussion on page 41) that every irreducible representation occurs as a component of the regular representation.

# Characters and Orthogonality Relations

Let $f$ and $g$ be complex valued functions on $G$. Define

$$(f,g) = \frac{1}{|G|} \sum_{\sigma \in G} f(\sigma)g(\sigma^{-1}).$$

This "inner product" is clearly bilinear, and is symmetric (i.e. $(f,g) = (g,f)$) since $\sigma$ can be replaced by $\sigma^{-1}$ in the sum.

**Proposition 6.1** *Let $\rho$ and $\rho'$ be inequivalent matrix representations of a finite group $G$. Then $(\rho_{ir}, \rho'_{sj}) = 0$ for all $i, r, s, j$. If $\rho$ is irreducible then $(\rho_{ir}, \rho_{sj}) = 0$ unless $i = j$ and $r = s$, in which case $(\rho_{ir}, \rho_{ri}) = 1/d$, where $d$ is the degree of $\rho$.*

**Proof:** Let $\rho : G \longrightarrow GL(V), \rho' : G \longrightarrow GL(V')$ be the given representations. Let $T : V \longrightarrow V'$ be a $\mathbf{C}$-linear map, and let $n = |G|$. Then $\frac{1}{n}F(T) = \frac{1}{n}\sum_{\sigma \in G} \sigma T \sigma^{-1}$ is a $G$-map from $V$ to $V'$. If $V$ and $V'$ are non-isomorphic and irreducible then $\frac{1}{n}F(T) = 0$ by Schur's Lemma. Choosing a basis and expressing this in terms of $\rho$ and $\rho\prime$, and letting $A$ be the matrix of $T$ with respect to the chosen basis gives

$$\frac{1}{n} \sum_{\sigma \in G} \rho'(\sigma) A \rho(\sigma^{-1}) = 0 \tag{6.1}$$

where $A$ can be any $d' \times d$ matrix, where $d = dim(V), d' = dim(V')$. Now let $A = E_{rs}$ be the elementary matrix with a 1 in the $(r,s)$ position and 0 elsewhere. One then checks that the $(i,j)$ entry of $\rho'(\sigma)E_{rs}\rho(\sigma^{-1})$ is $\rho'_{ir}(\sigma)\rho_{sj}(\sigma^{-1})$. Hence equation (6.1) implies that $\frac{1}{n}\sum_{\sigma \in G} \rho'_{ir}(\sigma)\rho_{sj}(\sigma^{-1}) =$

0; that is, $\frac{1}{n}(\rho'_{ir}, \rho_{sj}) = 0$ for all $i, r, s, j$. Since the 'inner product' is symmetric we are done.

Now suppose that $V$ is irreducible, so that $End_{\mathbf{C}[G]}(V) = \mathbf{C}$. Now $\frac{1}{n}\sum_\sigma \rho(\sigma)A\rho(\sigma^{-1}) = \lambda I$, where $\lambda$ depends on $A$ and $I$ is the identity matrix. Letting $A = e_{rs}$ and writing the corresponding $\lambda$ as $\lambda_{rs}$ gives

$$\frac{1}{n}\sum_\sigma \rho_{ir}(\sigma)\rho_{sj}(\sigma^{-1}) = \lambda_{rs}\delta_{ij} = 0 \quad \text{if } i \neq j$$

so that $(\rho_{ir}, \rho_{sj}) = 0$ if $i \neq j$. Similarly $(\rho_{sj}, \rho_{ir}) = 0$ if $s \neq r$. We also have that

$$\lambda_{rr} = (\rho_{ir}, \rho_{ri}) = (\rho_{ri}, \rho_{ir}) = \lambda_{ii}$$

and so there exists $\lambda$ with $\lambda_{ii} = \lambda$ for all $i$. Thus

$$\begin{aligned} d\lambda = \textstyle\sum_{i=1}^d \lambda_{ii} &= \tfrac{1}{n}\textstyle\sum_i \sum_\sigma \rho_{ri}(\sigma)\rho_{ir}(\sigma^{-1}) \\ &= \tfrac{1}{n}\textstyle\sum_\sigma \sum_i \rho_{ri}(\sigma)\rho_{ir}(\sigma^{-1}) \\ &= \tfrac{1}{n}\textstyle\sum_\sigma [\rho(\sigma)\rho(\sigma^{-1}]_{rr} \\ &= \tfrac{1}{n}\textstyle\sum_\sigma [I]_{rr} = \tfrac{1}{n}\cdot n = 1. \end{aligned}$$

Hence $\lambda = 1/d$ and we are done. □

We now introduce an extremely important tool in the study of representations.

**Definition:** The **character** of a representation $\rho : G \longrightarrow GL(V)$, denoted by $\chi(\rho)$ (or sometimes simply $\chi$), is defined to be $\chi(\sigma) = Tr[\rho(\sigma)]$ for $\sigma \in G$, where 'Tr' denotes the trace of a linear transformation. Note that $\chi$ can be computed the same way relative to any basis for $V$, since $Tr(ABA^{-1}) = Tr(B)$ for any $n \times n$ matrices $A$ and $B$ over $\mathbf{C}$. This also shows that $\chi$ is a class function, i.e. $\chi$ is a well-defined function on the conjugacy classes of $G$, and that equivalent representations have the same characters.

**Examples:**

1. Since the trivial representation $\rho : G \longrightarrow GL(V)$ is such that $\rho(g)$ is the $1 \times 1$ identity matrix for all $g \in G$, we see that $\chi(g) = 1$ for all $g \in G$.

2. If $\rho$ is the regular representation of $G$, choose the elements of $G$ as a basis for $\mathbf{C}[G]$. Let $\chi$ denote the character of $\rho$. Clearly $\chi(1) = |G|$, since multiplication by 1 is represented by the identity matrix with respect to the chosen basis. If $g \in G$ is not equal to 1, then $gh \neq h$ for all $h \in G$, hence the matrix representing multiplication by $g$ has zero's along the diagonal, so that $\chi(g) = 0$ in this case.

We will see other examples of characters later.

Note that if $\chi$ is a character of a representation of degree $n$ then $\chi(1) = n$. Also note that if $\chi$ and $\chi'$ are characters of representations $\rho : G \longrightarrow GL(V)$ and $\rho' : G \longrightarrow GL(V')$, respectively, then $\chi + \chi'$ is the character of the direct sum representation $\rho \oplus \rho' : G \longrightarrow GL(V \oplus V')$. In particular, the character of a representation $\rho$ is the sum of the characters of the irreducible components of $\rho$.

Characters play a central role in representation theory, as they encapsulate a great deal of information about their reprentations; indeed a character characterizes its representation. The following theorem shows that any two inequivalent irreducible representations are part of an orthonormal basis in the space of class functions on $G$. In fact, we will later see that the set of characters corresponding to the (finite number of) irreducible representations of $G$ forms an orthonormal basis for this function space.

**Theorem 6.2 (Orthogonality Relations)** *If $\rho$ and $\rho'$ are inequivalent representations with characters $\chi$ and $\chi'$, then $(\chi, \chi') = 0$. If $\rho$ is irreducible then $(\chi, \chi) = 1$.*

**Proof:** First note that $\chi(\sigma) = \sum_{i=1}^{d} \rho_{ii}(\sigma)$ and $\chi'(\sigma) = \sum_{i=1}^{d'} \rho'_{ii}(\sigma)$ for $\sigma \in G$. Then

$$(\chi, \chi') = (\sum_{i=1}^{d} \rho_{ii}, \sum_{j=1}^{d'} \rho'_{jj}) = \sum_{i=1}^{d} \sum_{j=1}^{d'} (\rho_{ii}, \rho'_{jj}) = 0$$

by bilinearity and by Proposition 6.1. For the same reasons we also have, if $\rho$ is irreducible, that

$$(\chi, \chi) = (\sum_{i=1}^{d} \rho_{ii}, \sum_{j=1}^{d} \rho_{jj}) = \sum_{i=1}^{d} \sum_{j=1}^{d} (\rho_{ii}, \rho_{jj}) = d \sum_{i=1}^{d} (\rho_{ii}, \rho_{ii}) = 1.$$

□

# The Group Ring

Let $G$ be a finite group. Recall Maschke's Theorem from Exercise 27 of Chapter 1 or Exercise 32 of Chapter 2, which tells us that the group algebra $\mathbf{C}[G]$ is semisimple. So $\mathbf{C}[G] \approx \prod_{i=1}^{r} \mathcal{M}_{d_i}(\mathbf{C})$. The multiplicity of an irreducible representation in the regular representation is precisely its degree $d_i$. We know from the Wedderburn theory (cf. the discussion on page 41) that $\mathbf{C}[G]$ has exactly $r$ isomorphism classes of simple modules, in other words $G$ has exactly $r$ inequivalent irreducible representations. The $d_i$'s are the degrees of the irreducible representations; hence $|G| = dim_{\mathbf{C}}(\mathbf{C}[G]) = \sum_{i=1}^{r} d_i^2$.

Is there some way to determine $r$, the number of inequivalent irreducible representations of $G$? The answer is yes; in fact $r$ is a familiar number associated to the group $G$.

**Proposition 6.3** *The number of inequivalent irreducible representations of a finite group $G$ is equal to the number of conjugacy classes in $G$.*

**Proof:** Let $R = \mathbf{C}[G]$, so that $R \approx \prod_{i=1}^{r} R_i$, where each $R_i$ is a matrix ring over a division $\mathbf{C}$-algebra of finite dimension. Hence $Z(R) = \prod_{i=1}^{r} Z(R_i)$, and each each $Z(R_i)$ is one-dimensional over $\mathbf{C}$ (remember that the center of a matrix ring over a field consists of scalar multiples of the identity matrix). Hence $r = dim_{\mathbf{C}}(Z(R))$.

Now let $x \in R$. Then $x \in Z(R)$ if and only if $\sigma x \sigma^{-1} = x$ for all $\sigma \in G$. Write $x = \sum_{\tau \in G} x_\tau \tau$. Then $x = \sigma x \sigma^{-1}$ is the same as

$$\begin{aligned}\textstyle\sum_{\tau \in G} x_\tau \tau &= \textstyle\sum_{\tau \in G} x_\tau \sigma \tau \sigma^{-1} \\ &= \textstyle\sum_{\tau \in G} x_{\sigma^{-1}\tau\sigma} \tau,\end{aligned}$$

so $x_\tau = x_{\sigma^{-1}\tau\sigma}$ for all $\sigma \in G$. Hence $x \in Z(R)$ if and only if $x_\tau = x_{\sigma^{-1}\tau\sigma}$ for all $\sigma \in G$. Let $\{C_j\}_{j=1}^{s}$ denote the conjugacy classes of $G$, and let $c_j = \sum_{\sigma \in C_j} \sigma$ in $\mathbf{C}[G]$. We shall call $c_j$ the **characteristic function** of the conjugacy class $C_j$. Clearly $\{c_j\}_{j=1}^{s}$ is a $\mathbf{C}$-basis for $Z(R)$, and so $r = dim_{\mathbf{C}}(Z(R))$ equals the number of conjugacy classes in $G$. □

**Examples:**

1. In Example 2 on Page 162 we found $n$ degree one representations (over $\mathbf{C}$)of the cyclic group $G = \mathbf{Z}/n\mathbf{Z}$. Note that these representations are pairwise inequivalent since they all have different characters. Since $G$ has $n$ conjugacy classes (each element is in its own class), Proposition 6.3 implies that these are precisely the irreducible representations of $G$.

2. Let $G = S_3$, the symmetric group on 3 letters. $S_3$ has 3 conjugacy classes, hence $S_3$ has 3 inequivalent irreducible representations. One of these is the trivial representation, which is of degree one; another is the degree one representation given by 'sgn', the sign of a permutation. One can check that these representations are inequivalent since their characters $\chi_1$ and $\chi_2$ take on different values on the odd permutations. So we know there is one more irreducible representation $\rho$ of $S_3$, and if $n$ is its degree then $1+1+n^2 = |S_3| = 6$, so $n = 2$. One can also figure out the values of the character $\chi_3$ of $\rho$ since $\chi_1 + \chi_2 + 2\chi_3$ is the character of the regular representation, which takes the value 0 on the non-identity elements of $G$ and the value $|G| = 6$ on the identity element.

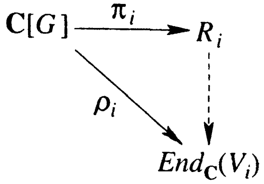
# Characters and Algebraic Integers

Note that in the decomposition $\mathbf{C}[G] = \prod_{i=1}^{r} R_i$ we can write $1 = \sum_{i=1}^{r} e_i$, where $e_i \in R_i$ is the unit in $R_i$ (i.e. the identity matrix in the matrix ring $R_i \approx \mathcal{M}_{d_i}(\mathbf{C})$). Then the $e_i$'s also form a basis for $Z(R) = \prod_{i=1}^{r} Z(R_i)$. Let $\rho_i$ correspond to an irreducible representation given by $R_i$. With $c_j$ denoting the characteristic function of the conjugacy class $C_j$ in $G$ (cf. the proof of Proposition 6.3), write

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_r$$

$$c_j = c_j^1 + c_j^2 + \cdots c_j^r.$$

Then $\rho_i(c_j) = \rho_i(c_j^i) = \lambda_j^i e_i$ for some $\lambda_j^i \in \mathbf{C}$ by Schur's Lemma. It should be noted that here we are identifying $\rho_i(c_j)$, which is an element of $End_{\mathbf{C}}(V_i)$, with an element of the group ring. Indeed the $\mathbf{C}[G]$-module structure on $V_i$, viewed as a ring map $\mathbf{C}[G] \longrightarrow End_{\mathbf{C}}(V_i)$, factors through the natural projection




Since $\rho_i(c_j^i) = \lambda_j^i e_i$, then $Tr(\rho_i(c_j)) = d_i \lambda_j^i$. On the other hand

$$Tr(\rho_i(c_j)) = \sum_{\sigma \in C_j} Tr(\rho_i(\sigma)) = h_j \chi_i(\sigma_j),$$

where $\sigma_j$ is any element of $C_j$, $h_j = |C_j|$ and $\chi_i$ is the character of $\rho_i$. Note that we've used the fact that a character $\chi$ of a representation is constant on conjugacy classes : $\chi(\sigma) = \chi(\tau\sigma\tau^{-1})$. This discussion shows that

$$\lambda_j^i = \frac{h_j \chi_i(\sigma_j)}{d_i}.$$

Our next goal is to show that the $\lambda_j^i$ are algebraic integers; that is, each satisfies some monic polynomial with coefficients in $\mathbf{Z}$.

**Theorem 6.4** *With notation as above, each $\lambda_j^i$ is an algebraic integer.*

**Proof:** Recall that $c_j$ is defined to be $\sum_{\sigma \in C_j} \sigma$, where $C_j$ is a conjugacy class in $G$. Hence $c_j c_k = \sum_{\sigma \in G} n_{jk\sigma}\sigma$, where $n_{jk\sigma}$ is a non-negative integer. Since $c_j c_k \in Z(\mathbf{C}[G])$, we have $\tau^{-1} c_j c_k \tau = c_j c_k$ for $\tau \in G$. This implies that

$$\begin{aligned} \textstyle\sum_{\sigma \in G} n_{jk\sigma}\sigma = c_j c_k &= \tau^{-1} c_j c_k \tau \\ &= \textstyle\sum_{\sigma \in G} n_{jk\sigma} \tau^{-1} \sigma \tau \\ &= \textstyle\sum_{\sigma \in G} n_{jk(\tau\sigma\tau^{-1})}\sigma \end{aligned}$$

so that $n_{jk\sigma} = n_{jk(\tau\sigma\tau^{-1})}$ for $\tau \in G$. Grouping terms in conjugacy classes gives $c_j c_k = \sum_{l=1}^{s} a_{jkl} c_l$ with $a_{jkl}$ a non-negative integer. Projecting onto the $i$th component gives :

$$(\lambda_j^i e_i)(\lambda_k^i e_i) = \rho_i(c_j)\rho_i(c_k) = \rho_i(c_j c_k) = \sum_{l=1}^{s} a_{jkl} \lambda_l^i e_i.$$

Hence $\lambda_j^i \lambda_k^i = \sum_{l=1}^{s} a_{jkl} \lambda_l^i$ with each $a_{jkl}$ a non-negative integer. By taking $M = \oplus_l \lambda_l^i \mathbf{Z}$ in the following proposition and by noting that $M$ is a faithful $\mathbf{Z}[\lambda_j^i]$-module for each $j$, we conclude that the $\lambda_j^i$ are algebraic integers.
□

**Proposition 6.5** *Let $A$ be a subring of a commutative ring $B$, and let $x \in B$. Then the following are equivalent:*

1. *$x$ is integral over $A$; that is, $x$ satisfies a monic polynomial with coefficients in $A$.*

2. *$A[x]$ is a finitely generated $A$-module.*

3. *$A[x]$ is contained in a subring $C$ of $B$ which is a finitely generated $A$-module.*

4. *There is a faithful $A[x]$-module $M$ which is finitely generated over $A$.*

**Proof:** It is obvious that (1) implies (2) and that (2) implies (3). The fact that (3) implies (4) is clear by taking $M = C$ and by noting that $1 \in C$. To prove that (4) implies (1), let $\{x_1, \ldots, x_n\}$ be a set of generators of $M$ as an $A$-module, and write $xx_i = \sum_{j=1}^{n} a_{ij}x_j$, that is

$$\sum_{j=1}^{n} x\delta_{ij}x_j = \sum_{j=1}^{n} a_{ij}x_j$$

or, written differently :

$$\sum_{j=1}^{n}(x\delta_{ij} - a_{ij})x_j = 0.$$

Let $P$ be the matrix $[p_{ij}]$ with $p_{ij} = x\delta_{ij} - a_{ij}$. So

$$P\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = 0.$$

Hence

$$det(P)\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = (adj(P))P\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = 0,$$

where $adj(P)$ denotes the adjoint matrix of $P$. Now $det(P)$ is a monic polynomial of degree $n$ in $x$ which acts trivially on $M$, and $det(P) = 0$ since $A[x]$ acts faithfully. □

We will need the following facts about algebraic integers, which henceforth we will use without comment. The proofs (with hints) are left for the exercise section at the end of this chapter.

1. Any rational number which is also an algebraic integer is in fact an integer.

2. The algebraic integers form a ring. More generally, if $A \subseteq B$ is an extension of commutative rings, the set of elements of $B$ which are integral over $A$ form a subring of $B$.

The fact that the $\lambda_j^i$ are algebraic integers has important consequences. Recall that the orthogonality relations tell us that if $\chi$ is the character corresponding to an irreducible representation, then $(\chi, \chi) = 1$. Thus, with $n = |G|$,

$$\frac{1}{n}\sum_{\sigma\in G}\chi_i(\sigma)\chi_i(\sigma^{-1})=1$$

Hence

$$\sum_{j=1}^{s}\frac{h_j\chi_i(\sigma_j)}{d_i}\chi_i(\sigma_j^{-1})=\frac{n}{d_i}$$

and so

$$\sum_{j=1}^{s}\lambda_j^i\chi_i(\sigma_j^{-1})=\frac{n}{d_i}.$$

Now $\sigma_j^k = 1$, where $k$ is the order of $\sigma_j$, so $\rho_i(\sigma_j)^k = 1$. Thus all the eigenvalues of $\rho_i(\sigma_j)$ are $k$th roots of unity. But $\chi_i(\sigma_j) = Tr(\rho_i(\sigma_j))$ is a sum of eigenvalues, hence is an algebraic integer, as is $\chi_i(\sigma_j^{-1})$. Thus $n/d_i$ is an algebraic integer. But $n/d_i \in \mathbf{Q}$, hence $n/d_i \in \mathbf{Z}$, or $d_i | n$. In other words, the degrees of the irreducible representations of a finite group divide the order of the group.

## Burnside's Theorem

In this section we use the tools of representation theory we have developed in this chapter to prove a famous theorem of Burnside. Burnside's Theorem was one of the first major theorems in group theory which was proved using representation theory.

With the notation as in the previous sections, let us recall we have shown so far:

1. $\lambda_j^i = \dfrac{h_j\chi_i(\sigma_j)}{d_i}$ is an algebraic integer (Theorem 6.4).
2. $\chi_i(\sigma_j)$ is an algebraic integer.
3. If $h_j$ and $d_i$ are relatively prime then $\dfrac{\chi_i(\sigma_j)}{d_i}$ is an algebraic integer. This follows from the following

**Lemma 6.6** *Let $a$ and $b$ be relatively prime integers. If $\alpha$ is an algebraic integer and if $a\alpha/b$ is an algebraic integer, then $\alpha/b$ is an algebraic integer.*

**Proof:** Since $a$ and $b$ are relatively prime, there exist $r, s \in \mathbf{Z}$ with $ra+sb = 1$. Hence $r(a\alpha/b) + s\alpha = \alpha/b$ and so $\alpha/b$ is an algebraic integer. □

**Lemma 6.7** *With notation as above, if $h_j$ and $d_i$ are relatively prime, then either $\rho_i(\sigma_j)$ is in the center of $\rho_i(G)$ or $\chi_i(\sigma_j) = 0$.*

**Proof:** First note that $\chi_i(\sigma_j) = Tr(\rho_i(\sigma_j))$ is the sum of $d_i$ roots of unity, so that $|\frac{\chi_i(\sigma_j)}{d_i}| \leq 1$. If equality holds then $|\chi_i(\sigma_j)| = d_i$, so that all of the eigenvalues of $\rho_i(\sigma_j)$ lie on the same ray through the origin. Since each eigenvalue also lies on the unit circle, they are all equal, so that $\rho_i(\sigma_j)$ is scalar and lies in the center of $\rho_i(G)$.

Now suppose that $|\frac{\chi_i(\sigma_j)}{d_i}| < 1$, and let $\alpha = \frac{\chi_i(\sigma_j)}{d_i}$. Let $\eta$ be a primitive $d_i$th root of unity and let $K = \mathbf{Q}(\eta)$. If $\sigma \in Gal(K/\mathbf{Q})$ then $\sigma(\alpha)$ is also $1/d_i$ times a sum of $d_i$ roots of unity., so that $|\sigma(\alpha)| \leq 1$. Hence $|\prod_{\sigma\in Gal(K/\mathbf{Q})} \sigma(\alpha)| < 1$. Since $\alpha$ is an algebraic integer, so is each $\sigma(\alpha)$, hence the product is an algebraic integer. Since the product is also a rational number, it must be an integer, hence it must be 0. But 0, being fixed by the Galois group, is its own (and only) galois conjugate, so that in fact $\alpha = 0$ and we are done. □

The core of Burnside's Theorem is contained in the following proposition, which in itself provides a nice condition under which a group is not simple.

**Proposition 6.8** *If the number of elements in some conjugacy class $C$ of a finite group $G$ is a positive power of a prime $p$, then there is a nontrivial irreducible representation $\rho$ of $G$ such that $\rho(C)$ is contained in the center of $\rho(G)$. In particular, $G$ is not simple.*

**Proof:** Let $\chi$ be the character of the regular representation of $G$. Then for all $1 \neq x \in G$, we have

$$0 = \chi(x) = \sum_{i=1}^{r} d_i\chi_i(x) = 1 + \sum_{i=2}^{r} d_i\chi_i(x) \tag{6.2}$$

With the notation as above, take $x = \sigma_j$. Then for a given $i$ either $p|d_i$ or $p \not| d_i$. If $p \not| d_i$ then $|C_j|$ and $d_i$ are clearly relatively prime, so by Lemma 6.7 we know that either $\rho_i(\sigma_j)$ is in the center of $\rho_i(G)$ or $\chi_i(\sigma_j) = 0$. Suppose the first alternative never happens for $i \geq 2$. Then by (Proposition 6.2) we have that $0 = 1 + p\beta$, where $\beta$ is an algebraic integer. But then $-1/p = \beta$ is an algebraic integer and a rational number, hence an integer (Exercise 12), an obvious contradiction. Thus $\rho_i(\sigma_j)$ is in the center of $\rho_i(G)$ for each $i$ and we are done. □

We are now ready to prove the main result of this chapter, Burnside's $p^aq^b$ Theorem, which states that every group of order $p^aq^b$ is solvable. It seems interesting that this purely group-theoretic result was not proven

without recourse to representation theory for nearly 60 years after Burnside's original 1904 proof, and even then the proof (by John Thompson) was quite long and complicated. This makes the proof using representation theory all the more impressive. A shorter purely group-theoretic proof of Burnside's Theorem was finally given by Goldschmidt ("A Group Theoretic Proof of the $p^a q^b$ Theorem, for Odd Primes") and Matsuyama ("Solvability of Groups of Order $2^a p^b$").

**Theorem 6.9 (Burnside's $p^a q^b$ Theorem)** *Every group of order $p^a q^b$, where $p$ and $q$ are distinct primes, is solvable.*

**Proof:** Let $G$ be a group of order $p^a q^b$. We proceed by induction on the order of $G$. First recall that groups of order $p^a$ are solvable (Exercise 16(a)). Choose a nontrivial element $x$ in the center of a $q$-Sylow subgroup of $G$. Then either $x \in Z(G)$ or $Con(x)$ - the conjugacy class of $x$ in $G$ - has (positive) prime power order (recall that $|Con(x)|$ is equal to the index of the centralizer of $x$ in $G$). Hence the hypothesis of Proposition 6.8 is satisfied, so that $G$ is not simple. The result follows by induction on the order of $G$, together with the standard result from group theory (Exercise 16b) that if $N$ is a normal subgroup of $G$ with both $N$ and $G/N$ solvable, then $G$ is solvable. □

Burnside's work originated in the problem of classifying finite simple groups, or at least finding restrictions on their orders. Finite simple groups have finally been classified, a culmination of decades of work by many mathematicians (Note: the proof is so huge, however, that its validity is still not wholly clear). Much of the progress in this area has been made using techniques of representation theory. Readers who are interested in the classification of finite simple groups should take a look at D. Gorenstein's book, *Finite Simple Groups.*

# Exercises

### Representations and Characters

1. Let $\chi$ be the character of a representation $\rho$. Prove that $\rho$ is irreducible if and only if $(\chi, \chi) = 1$.

2. Let $\chi$ be the character of a representation $\rho$. Show that the number of times that $\rho$ contains the trivial representation is equal to $(\chi, 1)$, where 1 denotes the character of the trivial representation.

3. Show that every character of $G$ which is 0 for all $1 \neq g \in G$ is an integral multiple of the character of the regular representation.

4. Prove that a finite group $N$ is abelian if and only if all irreducible representations of $N$ have degree 1. Conclude that if $N$ is an abelian subgroup of a finite group $G$ then every irreducible representation of $G$ has degree $\leq |G|/|N|$.

5. Let $G$ be a finite group and let $\rho$ be an irreducible representation of $G$ of degree $n$ with character $\chi$.

   (a) Prove that $|\chi(z)| = n$ for all $z \in Z(G)$, where $Z(G)$ denotes the center of $G$.

   (b) Prove that $n^2 \leq |G|/|Z(G)|$.

   (c) Prove that $Z(G)$ is cyclic if $\rho$ is faithful.

6. Let $\rho : G \longrightarrow GL(V)$ be a representation with character $\chi$, and let $V^*$ denote the dual space of $V$; that is, $V^*$ is the vector space of linear functionals on $V$. For $v \in V, v' \in V^*$, let $(v, v')$ denote the value of the linear functional $v'$ at $v$. Show that there exists a unique representation $\rho^* : G \longrightarrow GL(V^*)$ such that

$$(\rho(g)(v), \rho'(g)(v')) = (v, v') \quad \text{for } g \in G, v \in V, v' \in V^*.$$

   The representation $\rho'$ is called the **dual representation** of $\rho$. What is the character of the dual representation?

7. If $\rho : G \longrightarrow GL(V)$ and $\rho' : G' \longrightarrow GL(V')$ are representations then we may define a representation $\rho \otimes \rho' : G \times G' \longrightarrow GL(V) \otimes GL(V) \approx GL(V \otimes V')$ by

$$(\rho \times \rho')(g, g') = \rho(g) \otimes \rho'(g').$$

   This representation is called the **tensor product** of the representations $\rho$ and $\rho'$. We shall prove that $GL(V) \otimes GL(V)$ is isomorphic to $GL(V \otimes V)$ in Chapter 8.

   (a) If $\chi$, $\chi'$ and $\chi''$ are the characters of $\rho$, $\rho'$ and $\rho \otimes \rho'$ respectively, show that $\chi''(g, g') = \chi(g)\chi'(g')$ for all $(g, g') \in G \times G'$.

   (b) Show that if $\rho$ and $\rho'$ are irreducible then $\rho \otimes \rho'$ is irreducible.

   (c) Prove that every irreducible representation of $G \times G'$ is isomorphic to some representation of the form $\rho \otimes \rho'$, where $\rho$ and $\rho'$ are irreducible representations of $G$ and $G'$, respectively. This shows that the study of representations of a direct product can be reduced to the study of the representations of each of its factors.

8. When determining the values of the characters of the representations of $G$, it is a useful and common practice to make an array whose rows are indexed by these characters and whose columns are indexed by the conjugacy classes of $G$. The entry in the row indexed by the character $\chi_i$ and the column indexed by the conjugacy class $C_j$ is $\chi_i(C_j)$ (recall that characters are class functions). This table is called the **character table** of $G$.

   For each of the following groups $G$, determine the number of irreducible representations of $G$. Determine the character table of $G$.

   (a) $G = S_4$, the symmetric group on 4 letters.

   (b) $G = A_4$, the alternating group on 4 letters. Recall that $A_4$ is the subgroup of $S_4$ consisting of the set of even permutations.

   (c) $G = \{\pm 1, \pm i, \pm j, \pm k\}$, the multiplicative subgroup of order 8 in the quaternions. This is often called the quaternion group.

   (d) $G = D_n$, the dihedral group of order $2n$. Recall that $G$ is the group of rotations and reflections of the plane which preserve a regular polygon with $n$ vertices. If $r$ denotes a rotation through an angle of $2\pi/n$, and if $f$ (for 'flip') is any single reflection, then $G$ is generated by $r$ and $f$ with relations $r^n = f^2 = 1, frf = r^{-1}$. [Hint: The cases when $n$ is even or odd are different. Start by constructing the degree one and degree two representations.]

9. (a) Note that $D_4$ and the group $Q$ of quaternions have the same character table. Show that $D_4$ and $Q$ are not isomorphic, but the group algebras $\mathbf{C}[D_4]$ and $\mathbf{C}[Q]$ are isomorphic.

   (b) Show that the real group algebras $\mathbf{R}[D_4]$ and $\mathbf{R}[Q]$ are not isomorphic.

10. Prove that the number of degree one representations of a group $G$ is equal to $[G : G']$, where $G'$ denotes the commutator subgroup of $G$. Show how $G'$ can be determined from the character table of $G$.

11. (a) Let $G$ be a finite abelian group. Show that every irreducible complex representation of $G$ has degree one.

    (b)How many irreducible complex representations does $G$ have?

    (b) The group of characters of irreducible representations of a finite abelian group $G$ is called the **character group** of $G$. Prove that $G$ is isomorphic to its character group. [Hint : Write $G$ as a product of cyclic groups $G_1 \times \cdots \times G_n$, where each $G_i$ is generated by $g_i \in G_i$. Show that for any character $\chi$ as above, the value of $\chi$ on any element of one of $G_i$ is a $|G_i|$th root of unity. Now show that the homomorphism $f$ from the character group of $G$ to $G$ defined by $f(\chi) = (\chi(g_1), \ldots, \chi(g_n))$ is an isomorphism.]

### Algebraic Integers

12. Show that any rational number which is an algebraic integer is in fact an integer.

13. Show that the algebraic integers form a ring. More generally, show that if $A$ is a subring of a commutative ring $B$, then the set of elements of $B$ which are integral over $A$ forms a subring of $B$. [Hint: Use Proposition 6.5]

### Related to Burnside's Theorem

14. Let $G$ be a group having a faithful irreducible representation of degree $p^a$, with $a > 0$ and $p$ prime, and let $\chi$ be the character of that representation. Suppose $Z(G) = 1$, and let $H$ be a $p$-Sylow subgroup of $G$. Prove that $\chi(g) = 0$ for all $1 \neq g \in Z(H)$.

15. Prove that a nonabelian simple group cannot have a nilpotent subgroup of prime power index.

16. (a) Prove that any group whose order is a prime power is solvable. This begins the induction in Burnside's Theorem.

    (b) Let $N$ be a normal subgroup of a group $G$. Prove that $G$ is solvable if and only if both $N$ and $G/N$ are solvable. This allows one to use induction in the proof of Burnside's Theorem.

# 7

# The Global Dimension of a Ring

There is an invariant of rings called the global dimension. Semisimple rings are precisely those rings with global dimension zero. Thus the material in Chapters 1 and 2 can be considered the zero'th step in the theory of global dimension. Kaplansky, based upon an observation of Schanuel, was the first to set down the dimension theory of rings in an elementary way, without using the powerful machinery of homological algebra. This section is based on his Queen Mary College notes.

We saw in Chapter 1 that semisimple rings have a nice structure, namely they are all products of matrix rings over division rings. Theorem 1.18 shows that the semisimplicity of a ring $R$ is characterized by the property that every (left) $R$-module is projective; an instance of the phenomenon that the structure of a ring is reflected in the structure of modules over that ring. One way to measure how far an arbitrary ring $R$ is from being semisimple is to determine how far $R$-modules are from being projective. Let us begin, then, with a way of measuring how far a fixed $R$-module is from being projective.

**Definition:** Let $R$ be a ring and let $M$ be an $R$-module. A **(finite) projective resolution** is a long exact sequence

$$0 \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M$$

with each $P_i$ a projective $R$-module. The **projective dimension** of the module $M$, denoted $\boldsymbol{pd(M)}$, is the least $n$ for which there is a projective resolution as above; if no projective resolution for $M$ exists then we set $pd(M) = \infty$. Sometimes we denote projective dimension by $\boldsymbol{pd_R(M)}$ if we wish to emphasize that we are considering the dimension of $M$ as an $R$-module. Projective dimension is sometimes called **homological dimension**.

First note that $pd(M) = 0$ if and only if $M$ is projective; in this sense projective dimension gives a measure of how far a module is from being projective. We will see other evidence for this. It is also clear that $pd(M) = 1$ if and only if $M$ is not projective but is the quotient of two projective modules.

To compute the projective dimension of a module $M$ in practice, we need some way of telling when we actually have the smallest projective resolution of $M$ in hand. It is satisfying and useful that every projective resolution of $M$ has the same length, so that any projective resolution of $M$ may be used to compute its projective dimension. This follows from the following

**Lemma 7.1 (Schanuel's Lemma)** *Let $R$ be a ring and let*

$$0 \longrightarrow M \longrightarrow P \xrightarrow{f} N \longrightarrow 0$$

$$0 \longrightarrow M' \longrightarrow P' \xrightarrow{f'} N \longrightarrow 0$$

*be short exact sequences of $R$-modules. If $P$ and $P'$ are projective then $M \oplus P' \approx M' \oplus P$.*

**Proof:** Let $L = \{(x, x') \in P \oplus P' : f(x) = f'(x')\}$. Then it is easy to see that $L$ is a submodule of $P \oplus P'$ and that the natural projection $\pi : L \longrightarrow P$ is onto; for given $p \in P$, there exists $p' \in P'$ with $f'(p') = f(p)$ (since $f'$ is onto), and so $(p, p') \in L$ and $\pi(p, p') = p$. Since $P$ is projective, the surjective homomorphism $\pi : L \longrightarrow P$ splits, hence $L \approx ker(\pi) \oplus P$. But note that

$$ker(\pi) = \{(0, p') \in P \oplus P' : f'(p') = 0\} \approx ker(f') \approx M'$$

and so $L \approx M' \oplus P$. The same argument shows that $L \approx M \oplus P'$. □

An easy induction argument using Schanuel's Lemma shows that every projective resolution of a module $M$ has the same length, which is $pd(M)$. Instead of looking at long exact sequences, one can chop them up into short exact sequences to define projective dimension. $R$-modules $M$ and $M'$ are said to be **projectively equivalent** if there are projective $R$-modules $P$ and $P'$ with $M \oplus P \approx M' \oplus P'$. It is not difficult to check that this is actually an equivalence relation; we denote the equivalence class of $M$ by $[M]$. It follows from Schanuel's Lemma that if

$$0 \longrightarrow N \longrightarrow P \longrightarrow M \longrightarrow 0$$

and

$$0 \longrightarrow N' \longrightarrow P' \longrightarrow M' \longrightarrow 0$$

are short exact sequences with $P$ and $P'$ projective, then $[M] = [M']$ implies $[N] = [N']$. Now if $M$ is any $R$-module then we can map a projective $R$-module $P$ onto $M$ with kernel $N$ as above. Defining a map $\mathcal{R}$ by $\mathcal{R}([M]) = [N]$, this discussion shows that $\mathcal{R}$ is well-defined. It is easy to check that $pd(M)$ is the smallest integer $n$ with $\mathcal{R}^n([M]) = 0$.

Note also that if we have an exact sequence $0 \longrightarrow N \longrightarrow P \longrightarrow M \longrightarrow 0$ with $P$ projective, then $\mathcal{R}^n([M]) = \mathcal{R}^{n-1}([N])$ for all $n \geq 1$. This shows

that $pd(N) = 0$ if $pd(M) = 0$, $pd(M) = \infty$ if and only if $pd(N) = \infty$, and $pd(N) = pd(M) - 1$ if $pd(M) > 0$.

**Examples:**

1. $pd_F(V) = 0$ for any vector space $V$ over a field $F$, since any such $V$ is a free $F$-module.

2. If $G$ is an abelian group then $pd_{\mathbf{Z}}(G) = 0$ if $G$ is free abelian and $pd_{\mathbf{Z}}(G) = 1$ if $G$ is not free. The first fact is clear, the second follows from the exact sequence

$$0 \longrightarrow \mathbf{Z} \longrightarrow \mathbf{Z} \longrightarrow \mathbf{Z}/n\mathbf{Z} \longrightarrow 0.$$

3. Let $p$ be prime and consider the ring $R = \mathbf{Z}/p^2\mathbf{Z}$. The annihilator of $p \in R$ is the ideal $pR$, so we have an exact sequence

$$0 \longrightarrow pR \longrightarrow R \longrightarrow pR \longrightarrow 0$$

of $R$-modules. But $pR$ is not projective, for otherwise $p$ would generate $R$. The discussion above shows that $\mathcal{R}([pR]) = [pR]$; hence $pd_R(pR) = \infty$.

4. Example 3 immediately generalizes to the following: Let $a, b \in R$ be such that $ann(a) = bR$ and $ann(b) = aR$. Then either $pd(aR) = pd(bR) = \infty$ or $aR \oplus bR \approx R$ as $R$-modules and $pd(aR) = pd(bR) = 0$.

5. If $\{M_i\}$ is any collection of $R$-modules, then $pd(\bigoplus M_i) = sup\{pd(M_i)\}$.

Having a measure of how far a module is from being projective gives a natural way of measuring how far a ring is from being semisimple.

**Definition:** The (left) **global dimension** of a ring $R$, denoted $\boldsymbol{gd(R)}$, is defined to be the supremum of the projective dimensions of left $R$-modules:

$$gd(R) = sup\{pd_R(M) : M \text{ a left } R\text{-module}\}.$$

**Examples:**

1. $gd(R) = 0$ if and only if $R$ is semisimple. This follows from the fact (Theorem 1.18) that $R$ is semisimple if and only if every (left) $R$-module is projective; and an $R$-module $M$ is projective if and only if $pd(M) = 0$.

2. A ring is said to be a **(left) hereditary ring** if all of its left ideals are projective as $R$-modules. Hence $gd(R) = 1$ if and only if $R$ is a hereditary ring which is not semisimple. Hereditary rings have been studied extensively by ring theorists. For more on hereditary rings, see the exercises at the end of this chapter.

There is an obvious way of defining (right) projective dimension for right $R$-modules, which gives rise to the notion of right global dimension for the ring $R$. Since, by Corollary 1.12, a ring is left semisimple if and only if it is right semisimple, we see that a ring has left global dimension zero if and only if it has right global dimension zero. This statement does not hold true in general, however: there exist rings whose left and right global dimensions are not equal (see Exercise 11). In what follows we will always be working with left global dimension, although the statements would hold for right global dimension as well.

**Lemma 7.2** *Let* $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ *be an exact sequence of R-modules. If any two of these modules has finite projective dimension, then so does the third, in which case*

$$\begin{aligned} pd(A) &\leq max\{pd(B), pd(C)\} \\ pd(B) &\leq max\{pd(A)+1, pd(C)\} \\ pd(C) &\leq max\{pd(A)+1, pd(B)+1\} \end{aligned}$$

*Furthermore, if* $pd(B) = 1$ *and* $pd(C) > 1$, *then* $pd(C) = pd(A) + 1$.

**Proof:** We prove only the first half of the lemma as this is the only part which will be needed later; the proof of the second half is left to the reader.

We induct on the sum of the given two dimensions. If $C$ is projective then the sequence splits and $B \approx A \oplus C$, so $[B] = [A]$ and $pd(B) = pd(A)$. If $B$ is projective then $\mathcal{R}([C]) = [A]$, so that $pd(a) \leq c \leq a+1$ and the result holds. So suppose that neither $B$ nor $C$ is projective.

Map a projective module $P$ onto $B$ with kernel $D$. Let $E$ be the preimage under this map of $A \subseteq B$. Note that $E$ is equal to the kernel of the epimorphism $P \longrightarrow B \longrightarrow C$, and that $D$ and $E$ are projective. It is easy to check that the sequences

$$0 \longrightarrow D \longrightarrow P \longrightarrow B \longrightarrow 0$$

$$0 \longrightarrow E \longrightarrow P \longrightarrow C \longrightarrow 0$$

$$0 \longrightarrow D \longrightarrow E \longrightarrow A \longrightarrow 0$$

are exact. Since $pd(B) \neq 0$ and $pd(C) \neq 0$ we have that $pd(D) = pd(B) - 1$ and $pd(E) = pd(C) - 1$, so that at least two of the modules in the third

exact sequence above have finite projective dimensions whose sum is less than the sum in the original sequence. The result follows by induction: for example $pd(E) \leq max\{pd(D)+1, pd(A)\}$ implies that $pd(C) \leq \{pd(B)+1, pd(A)+1\}$; the other two inequalities follow similarly. □

The following proposition is due to Kaplansky.

**Proposition 7.3** *Let $R$ be a ring and let $a \in R$ be an element in the center of $R$ which is not a zero-divisor. If $M$ is a nonzero $R/(a)$-module then $pd_R(M) = pd_{R/(a)}(M) + 1$.*

**Proof:** We induct on $n = pd_{R/(a)}(M)$. If $n = 0$ then $M$ is a projective $R/(a)$-module, hence a direct summand of some free $R/(a)$-module $N$. Since $(a)$ is a free $R$-module and is not a direct summand of $R$, we have $pd_R(R/(a)) = 1$ and $pd_R(N) = 1$; hence $pd_R(M) \leq 1$. To show that $M$ is not a projective $R$-module, note that $a$ acts faithfully on any free $R$-module, and thus on any non-zero projective $R$-module.

Now assume $n > 0$, and map a free $R/(a)$-module $N$ onto $M$ to form

$$0 \longrightarrow L \longrightarrow N \longrightarrow M \longrightarrow 0.$$

Then $L \neq 0$ and $pd_{R/(a)}(L) = n-1$, so $pd_R(L) = n$ by induction. Also note that $pd_R(N) = 1$. It follows from Lemma 7.2 that $pd_R(M) \leq n+1$, with equality if $n > 1$. If $n = 1$ write $M = P/Q$ for $R$-modules $P$ and $Q$ with $P$ projective. Then we have the following exact sequences of $R/(a)$-modules (note that $aM = 0$ so $aP \subseteq Q$):

$$0 \longrightarrow Q/aP \longrightarrow P/aP \longrightarrow M \longrightarrow 0$$

$$0 \longrightarrow aP/aQ \longrightarrow Q/aQ \longrightarrow Q/aP \longrightarrow 0.$$

Since $P/aP$ is a projective $R/(a)$-module and since $n = 1$, we have that $Q/Pa$ is a projective $R/(a)$-module, so the second exact sequence splits. Thus $M \approx aP/aQ$ is a direct summand of $Q/aQ$, which is therefore not projective. Hence $Q$ is not a projective $R$-module, and $pd_R(M) > 1$, completing the proof. □

An immediate consequence of Proposition 7.3 is the following

**Corollary 7.4** *Let $R$ be a ring and let $a \in R$ be an element in the center of $R$ which is not a zero-divisor. If $gd(R/(a)) = n < \infty$ then $gd(R) \geq n+1$.*

Corollary 7.4 can be used to help compute the global dimension of a polynomial ring in terms of the global dimension of its ring of coefficients.

**Theorem 7.5** *Let $R[x]$ be the polynomial ring over the ring $R$. Then $gd(R[x]) = gd(R) + 1$.*

**Proof:** We give the argument for $gd(R) < \infty$; the case $gd(R) = \infty$ is not much different and is left to the reader. It follows immediately from Corollary 7.4 that $gd(R[x]) \geq gd(R) + 1$.

We now show that the inequality also goes in the reverse direction; that is, $pd_{R[x]}(M) \leq pd_R(M) + 1$ for every $R$-module $M$. The first thing to note is that $pd_R(M) = pd_{R[x]}(R[x] \otimes_R M)$. One direction follows from the fact that $R[x] \otimes M$ is a projective $R$-module if $M$ is a projective $R$-module, which is easy to see since the same statement clearly holds for free modules and since direct sums distribute through tensor products. Conversely, if $R[x] \otimes M$ is $R[x]$-projective, then $R[x] \otimes M$ is a direct summand of some free $R[x]$-module, which is also a free $R$-module; hence $R[x] \otimes M$ is $R$-projective. But as an $R$-module, $R[x] \otimes M$ is just a sum of copies of $M$, so $M$ is $R$-projective. It follows that $pd_R(M) = pd_{R[x]}(R[x] \otimes_R M)$.

Now $R[x]$ acts on both $R[x]$ and $M$. Taking the difference of these two actions gives a map

$$\psi : R[x] \otimes M \longrightarrow R[x] \otimes M$$
$$\sum_i x^i \otimes m_i \mapsto \sum_i (x^{i+1} \otimes m_i - x^i \otimes xm_i).$$

Let $\mu : R[x] \otimes M \longrightarrow M$ be the multiplication map induced by $\mu(f \otimes m) = fm$. Then there is an exact sequence of $R[x]$-modules

$$0 \longrightarrow R[x] \otimes M \xrightarrow{\psi} R[x] \otimes M \xrightarrow{\mu} M \longrightarrow 0.$$

Lemma 7.2 then implies that $pd_{R[x]}(M) \leq pd_{R[x]}(R[x] \otimes M) + 1 = pd_R(M) + 1$. □

An immediate corollary is the famous

**Corollary 7.6 (Hilbert Syzygy Theorem)** *Let $k[x_1, \ldots, x_n]$ be a polynomial ring in $n$ variables over a field $k$. Then $gd(k[x_1, \ldots, x_n]) = n$.*

# Exercises

1. Use Schanuel's Lemma to show that every projective resolution of an $R$-module has the same length.

2. (a) Recall that two $R$-modules $M$ and $M'$ are called **projectively equivalent** if there are projective $R$-modules $P$ and $P'$ with $M \oplus P \approx M' \oplus P'$. Show that this is an equivalence relation.

   (b) With the notation as on page 178, show that $pd(M)$ is the smallest integer $n$ with $\mathcal{R}^n([M]) = 0$.

3. State and prove a dual version to Schanuel's Lemma.

4. Let $a, b \in R$ be such that $ann(a) = bR$ and $ann(b) = aR$. Show that either $pd(aR) = pd(bR) = \infty$ or $aR \oplus bR \approx R$ as $R$-modules and $pd(aR) = pd(bR) = 0$.

5. Show that if $\{M_i\}$ is any collection of $R$-modules, then $pd(\bigoplus M_i) = sup\{pd(M_i)\}$.

6. Prove the second half of Lemma 7.2.

7. Let $R$ be a commutative ring, $M$ an $R$-module, and $A$ a free $R$-algebra. Show that the projective dimension of $M$ as an $R$-module is equal to the projective dimension of $M$ as an $A$-module.

8. Prove that $gd(\mathcal{M}_n(R)) = gd(R)$ for any ring $R$.

9. (D.E. Cohen) Let $S$ be a subring of $R$ such that $S$ is a direct summand of $R$ as an $R-S$ bimodule. Prove that $gd(S) \leq gd(R) + pd_S(R)$. In particular, if $R$ is projective as ans $S$-module then $gd(S) \leq gd(R)$. [Hint: If $M$ is an $S$-module, first show that $pd(M) \leq pd(Hom_S(R, M))$.]

10. (a) Let $R[x, x^{-1}]$ be the ring of Laurent series over the ring $R$. What is the relationship between $gd(R[x, x^{-1}])$ and $gd(R)$? Prove it.

    (b) Use part (a) to derive a result for Laurent series in many variables which is analogous to the Hilbert Syzygy Theorem.

11. (Small) Let $R$ be the ring of matrices $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ with $a \in \mathbf{Z}, b, c \in \mathbf{Q}$. Show that $R$ has left global dimension 1 but right global dimension 2.

    **Remark:** In fact, Jategaonkar proved that if $1 \leq m < n \leq \infty$, then there exists a ring $R$ with left global dimension $m$ and right global dimension $n$. See his paper "A counter-example in ring theory and homological algebra", *J. Algebra* 12 (1969), pp.418-440.

12. Show that semisimple rings, principal ideal domains, and the ring of upper triangular matrices of a division ring are hereditary.

13. (Cartan-Eilenberg)

    (a) Show that if $R$ is a hereditary ring, then every submodule of a free $R$-module is isomorphic to a direct sum of (left) ideals.

    (b) Prove that a ring $R$ is hereditary if and only if every submodule of a projective $R$-module is projective.

    (c) Prove that a ring $R$ is hereditary if and only if every quotient module of an injective $R$-module is injective.

# 8

# The Brauer Group of a Commutative Ring

An absolutely natural impulse in virtually all of algebra is to do for commutative rings what has already been done for fields.

*D. Zelinsky*

The Brauer group $Br(R)$ of a commutative ring was introduced by Auslander and Goldman in their 1960 paper *The Brauer Group of a Commutative Ring*, building on earlier work of Azumaya. This group coincides with the "classical" Brauer group (cf. Chapter 4) in the case when $R$ is a field. One of the points of extending the theory to rings is that one can relate Brauer groups of fields to Brauer groups of related rings in exact sequences; one then hopes that this will help compute the classical Brauer group. The Brauer group of a commutative ring is also part of a Galois theory of commutative rings. For more on these matters, the reader may consult *Galois Theory and Cohomology of Commutative Rings* by Chase, Harrison and Rosenberg, *The Brauer Group of Commutative Rings* by Orzech and Small, *Separable Algebras Over Commutative Rings* by DeMeyer and Ingraham, or the paper of Auslander and Goldman quoted above.

Henceforth, unless otherwise specified, $R$ will denote a commutative ring and all (unlabeled) tensoring will be done over $R$.

## Azumaya Algebras

In this section we introduce the notion of Azumaya algebra over a commutative ring, which generalizes the notion of central simple algebra over a field. Just as in the case of fields, these objects will be central to our study; in particular we will form a group out of the set of (equivalence classes of) Azumaya algebras over a fixed ring $R$.

**Definition:** Let $A$ be an $R$-algebra. Let $A^e = A \otimes_R A^\circ$, where $A^\circ$ denotes the opposite algebra of $A$. The $R$-algebra $A^e$ is called the **enveloping algebra** of $A$.

There is a natural homomorphism $\psi : A^e \longrightarrow End_R(A)$ defined by

$$\psi(a \otimes \alpha)(y) = ay\alpha$$

extended linearly. Recall from Chapter 0, Exercise 28 that there is a one-to-one correspondence between left $A^e$-modules and A-A bimodules.

**Definition:** An $R$-module $A$ is said to be **faithfully projective** if $A$ is finitely generated, projective and faithful as an $R$-module. An $R$-algebra $A$ is called an **Azumaya algebra** if the following two conditions hold:

1. $A$ is a faithfully projective $R$-module.
2. The map $\psi : A^e \longrightarrow End_R(A)$ defined above is an isomorphism.

**Example:** If $k$ is a field then a (finite dimensional) $k$-algebra $A$ is an Azumaya algebra if and only if $A$ is central simple. For suppose that $A$ is central simple. Then $A$ is faithfully projective since $k$ is a field, and Proposition 3.12 shows that condition (2) above is satisfied. Hence any central simple algebra over a field is an Azumaya algebra.

Conversely, if $A$ is an Azumaya $k$-algebra, then $A \approx k^n$ as $k$-modules for some $n$ since $A$ is faithfully projective. From this fact and condition (2) in the definition of Azumaya algebra we see that

$$A^e \approx End_k(A) \approx End_k(k^n) \approx \mathcal{M}_n(k)$$

so that $A^e$ is a central simple $k$-algebra. But for any $k$-algebras $A$ and $B$, both $A$ and $B$ are central simple if $A \otimes B$ is central simple; hence $A$ is central simple since $A^e \approx A \otimes A^\circ$ is central simple.

We will see other examples of Azumaya algebras later.

Theorems about endomorphism algebras of projective $R$-modules can often be reduced to similar questions about endomorphism algebras of free $R$-modules, a fact which we shall often exploit. Hence we begin with a proposition describing the behavior of matrix algebras under the tensor product.

**Proposition 8.1** *Let $R$ be a commutative ring. Then*

1. $\mathcal{M}_m(R) \otimes \mathcal{M}_n(R) \approx \mathcal{M}_{mn}(R)$.
2. *The map $w : End_R(R^m) \otimes End_R(R^n) \longrightarrow End_R(R^m \otimes R^n)$ defined by $w(f \otimes g) = f \otimes g$ extended linearly is an isomorphism of $R$-algebras.*

**Proof:** Let $\{e_1, \ldots, e_m\}$ be a basis for $R^m$ and let $\{f_1, \ldots, f_n\}$ be a basis for $R^n$. Then $R^m \otimes R^n$ has basis $\{e_i \otimes f_j : 1 \le i \le m, 1 \le j \le n\}$. Let $E_{ij} \in End_R(R^m)$ and $F_{kl} \in End_R(R^n)$ be defined by

$$E_{ij}(e_r) = \delta_{ir} e_j, \quad 1 \le i, j, r \le m$$

$$F_{kl}(f_s) = \delta_{ks} f_l, \quad 1 \le k, l, s \le n$$

where $\delta_{ir}$ equals 1 when $i = r$ and is 0 when $i \ne r$. Then $\{E_{ij} : 1 \le i, j \le m\}$ is an $R$-algebra basis for $End_R(R^m)$ and $\{F_{kl} : 1 \le k, l \le n\}$ is an $R$-algebra basis for $End_R(R^n)$, so that $\{E_{ij} \otimes F_{kl} : 1 \le i, j \le m; 1 \le k, l \le n\}$ is an $R$-algebra basis for $End_R(R^m) \otimes End_R(R^n)$.

Let $h \in End_R(R^m \otimes R^n)$ be given. Then

$$h(e_i \otimes f_j) = \sum_{k,l} h_{ik,jl} e_k \otimes f_l$$

for some $h_{ik,jl} \in R$. Let $h' = \sum_{k,l} h_{ik,jl} E_{ik} \otimes F_{jl}$. Then it is easy to check that $w(h') = h$; hence $w$ is surjective. To show that $w$ is injective, first note that any element $h \in End_R(R^m) \otimes End_R(R^n)$ can be written uniquely as $h = \sum_{i,j,k,l} h_{ij,kl} E_{ij} \otimes F_{kl}$. We now compute

$$\begin{aligned} w(h)(e_\sigma \otimes f_\tau) &= \textstyle\sum_{i,j,k,l} h_{ij,kl} E_{ij}(e_\sigma) \otimes F_{kl}(f_\tau) \\ &= \textstyle\sum_{i,j,k,l} h_{ij,kl} (\delta_{i\sigma} e_j \otimes \delta_{k\tau} f_l) \\ &= \textstyle\sum_{j,l} h_{\sigma j,\tau l} e_j \otimes f_l. \end{aligned}$$

If $w(h) = 0$ then $w(h)(e_\sigma \otimes f_\tau) = 0$ for each $\sigma, \tau$. Since $\{e_j \otimes f_l\}$ forms a basis for $R^m \otimes R^n$, the above computation implies that $h_{\sigma j,\tau l} = 0$ for all $\sigma, \tau, j, l$; hence $h = 0$. □

A more general version of Proposition 8.1 is given in Exercise 2.

Recall from Exercise 10 of Chapter 0 that if $E_1, \ldots, E_n, F_1, \ldots, F_m$ are any $R$-modules and $\phi : E_1 \oplus \cdots \oplus E_n \longrightarrow F_1 \oplus \cdots \oplus F_m$ is a $R$-module homomorphism, then $\phi$ can be represented by a unique matrix

$$M(\phi) = \begin{bmatrix} \phi_{11} & \cdots & \phi_{1n} \\ \vdots & & \vdots \\ \phi_{m1} & \cdots & \phi_{mn} \end{bmatrix}$$

where $\phi_{ij} \in Hom_R(E_j, F_i)$. In particular, for $R$-modules $M$ and $N$, there are homomorphisms

$$End_R(M) \xrightarrow{i} End_R(M \oplus N) \xrightarrow{j} End_R(M)$$

$$f \overset{i}{\longmapsto} \begin{bmatrix} f & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} x & y \\ z & w \end{bmatrix} \overset{j}{\longmapsto} x$$

Notice that $j \circ i$ is the identity, so that $i$ is injective and $j$ is surjective. We shall use this observation several times in what follows. The recurring theme will be that projective modules are direct summands of free modules, whose endomorphism algebras we understand quite well, so we should be able to use the above maps to tell us something about endomorphism algebras of projective modules. We begin with a useful illustration of this idea.

**Proposition 8.2** *If $P$ and $Q$ are finitely generated projective $R$-modules then the map $w : End_R(P) \otimes End_R(Q) \longrightarrow End_R(P \otimes Q)$ defined by $w(f \otimes g) = f \otimes g$ extended linearly is an isomorphism.*

**Proof:** As $P$ and $Q$ are finitely generated projective $R$-modules, we can choose $R$-modules $P'$ and $Q'$ with $P \oplus P' \approx R^n$ and $Q \oplus Q' \approx R^m$. We then have the the following commutative diagram:

$$\begin{array}{ccc}
End_R(P) \otimes End_R(Q) & \xrightarrow{\quad w \quad} & End_R(P \otimes Q) \\
{\scriptstyle i}\big\downarrow \big\uparrow{\scriptstyle j} & & {\scriptstyle i'}\big\downarrow \big\uparrow{\scriptstyle j'} \\
End_R(P \oplus P') \otimes End_R(Q \oplus Q') & & End_R((P \oplus P') \otimes (Q \oplus Q')) \\
\approx \big\downarrow & & \big\downarrow \approx \\
End_R(R^n) \otimes End_R(R^m) & \xrightarrow{\quad w' \quad} & End_R(R^n \otimes R^m)
\end{array}$$

where the homomorphism $i$ and its splitting homomorphism $j$ are induced by the inclusions $P \hookrightarrow P \oplus P'$ and $Q \hookrightarrow Q \oplus Q'$, as discussed above; similarly $i'$ and $j'$ are induced by these inclusions. The bottom right-hand side isomorphism comes from the fact that

$$(P \oplus P') \otimes (Q \otimes Q') \approx (P \otimes Q) \oplus (P \otimes Q') \oplus (P' \otimes Q) \oplus (P' \otimes Q')$$

and since $P \oplus P' \approx R^n$ and $Q \oplus Q' \approx R^m$. Note that the diagram above commutes, including the splitting maps. Since $w'$ is an isomorphism by Proposition 8.1, it follows that $w$ is an isomorphism. □

Just as matrix algebras with entries in a field $k$ played an important role in the study of $Br(k)$ (namely, these are precisely the algebras representing $[k] = 1 \in Br(k)$), so shall $End_R(P)$ for faithfully projective $R$-modules $P$ play an important role in $Br(R)$. The first basic fact about these endomorphism algebras is that they are Azumaya algebras.

**Proposition 8.3** *If $P$ is a faithfully projective $R$-module then $End_R(P)$ is an Azumaya $R$-algebra.*

**Proof:** Since $P$ is a finitely generated projective $R$-module, there is an $R$-module $Q$ with $P \oplus Q \approx R^n$ for some $n$. Hence $End_R(P \oplus Q) \approx End_R(R^n) \approx \mathcal{M}_n(R) \approx R^{n^2}$ as $R$-modules, so that $End_R(P \oplus Q)$ is free. But by the discussion on page 187, there are homomorphisms $End_R(P) \longrightarrow End_R(P \oplus Q) \longrightarrow End_R(P)$ whose composition is the identity; hence $End_R(P)$ is finitely generated projective. If $r \in R$ annihilated $End_R(P)$, then in particular it would annihilate the identity map $1 \in End_R(P)$, whence it would annihilate $P$. Since $P$ is a faithful $R$-module, this shows that $End_R(P)$ is a faithful $R$-module.

It is left to prove that $End_R(P)$ satisfies condition (2) in the definition of Azumaya algebra. Let $Q$ be as above, so that $P \oplus Q \approx R^n$. Then it is not difficult to check that the following diagram commutes:

$$\begin{array}{ccc}
End_R(P) \otimes End_R(P)^\circ & \xrightarrow{\ \psi_P\ } & End_R(End_R(P)) \\
\downarrow \uparrow & & \downarrow \uparrow \\
End_R(P \oplus Q) \otimes End_R(P \oplus Q)^\circ & \xrightarrow{\ \psi_{P \oplus Q}\ } & End_R(End_R(P \oplus Q))
\end{array}$$

where, as always, the vertical maps and their splittings are induced by the inclusion $P \hookrightarrow P \oplus Q$, and the horizontal homomorphisms are as in condition (2) of the definition of Azumaya algebra. Hence to show that $\psi_P$ is an isomorphism it suffices to show that $\psi_{P \oplus Q}$ is an isomorphism.

Let $\{e_1, \ldots, e_n\}$ be a basis for the free $R$-algebra $P \oplus Q \approx R^n$, and let $E_{ij} \in End_R(R^n)$ be defined by $E_{ij}(e_k) = \delta_{ik} e_j$. Then $\{E_{ij} : 1 \le i, j \le n\}$ is an $R$-algebra basis for $End_R(R^n)$, and $\{E_{ij} \otimes E_{kl} : 1 \le i, j, k, l \le n\}$ is an $R$-algebra basis for $End_R(R^n) \otimes End_R(R^n)^\circ$. We also have, by definition of $\psi_{P \oplus Q}$, that

$$\psi_{P\oplus Q}(E_{ij}\otimes E_{kl})(E_{st}) = E_{ij}E_{st}E_{kl} = \delta_{js}\delta_{tk}E_{il}.$$

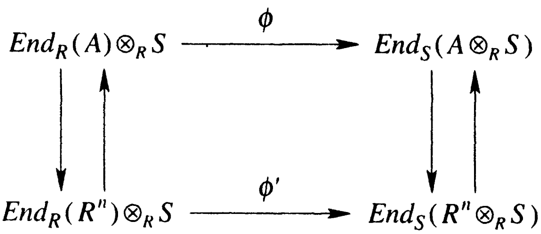
From this it is easy to check that $\psi_{P\oplus Q}$ is an isomorphism. □

The Brauer group of a commutative ring $R$ will consist of (equivalence classes of) Azumaya algebras over $R$ with the tensor product as the group operation. The following proposition will help show that the group is close under this operation.

**Proposition 8.4** *If $A$ and $B$ are Azumaya algebras then $A \otimes B$ is an Azumaya algebra.*

**Proof:** We leave as an exercise for the reader the fact that $A\otimes B$ is faithfully projective if both $A$ and $B$ are faithfully projective (Exercise 3).

Now let $\psi_{A\otimes B} : (A\otimes B)^e \longrightarrow End_R(A\otimes B)$ be the homomorphism defined in condition (2) of the definition of Azumaya algebra. Then the following diagram is commutative:




Here $\psi_A : A\otimes_R A^\circ \longrightarrow End_R(A)$ denotes the isomorphism coming from the fact that $A$ is Azumaya (similarly for $\psi_B$), $w$ is the isomorphism given by Proposition 8.1, and the left side vertical isomorphism comes from the commutativity of the tensor product and the fact that $(A\otimes B)^\circ \approx A^\circ\otimes B^\circ$. This shows that $\psi_{A\otimes B}$ is an isomorphism. Hence $A\otimes B$ is an Azumaya $R$-algebra. □

A subject intimately connected with Azumaya algebras is that of Polynomial Identity Rings. An explanation of this relationship can be found in L. Rowen, Ring Theory, Vol. II, Chapter 6.

# Constructing the Brauer group

In this section we define the Brauer group of a commutative ring and prove that $Br(\ )$ is functorial.

In our study of the Brauer group of a commutative ring, we will introduce an equivalence relation on the set of Azumaya algebras over that ring, just as in the case for fields. More precisely, we make the following

**Definition:** Let $A$ and $B$ be Azumaya algebras over $R$. We write $A \sim B$ if there exist faithfully projective $R$-modules $P$ and $Q$ such that $A \otimes_R End_R(P) \approx B \otimes_R End_R(Q)$.

Note that in the case when $R$ is a field, $\sim$ is precisely the equivalence relation on central simple algebras over $R$ which was introduced in Chapter 4 on page 110. The equivalence classes of central simple $R$-algebras under that relation form the elements of the Brauer group $Br(R)$ of the field $R$.

Proposition 8.2 can be used to show that $\sim$ is indeed an equivalence relation. The only thing to check is transitivity, so suppose that $A \sim B$ and $B \sim C$ for Azumaya algebras $A, B, C$ over $R$. Then there exist faithfully projective $R$-modules $P, P', Q, Q'$ with

$$A \otimes End_R(P) \approx B \otimes End_R(Q)$$

$$B \otimes End_R(P') \approx C \otimes End_R(Q').$$

This implies that

$$\begin{aligned} A \otimes End_R(P \otimes P') &\approx A \otimes End_R(P) \otimes End_R(P') \\ &\approx B \otimes End_R(Q) \otimes End_R(P') \\ &\approx B \otimes End_R(P') \otimes End_R(Q) \\ &\approx C \otimes End_R(Q') \otimes End_R(Q) \\ &\approx C \otimes End_R(Q' \otimes Q) \end{aligned}$$

with $P \otimes P'$ and $Q' \otimes Q$ faithfully projective since $P, P', Q, Q'$ are faithfully projective (Exercise 3); hence $A \sim C$.

With this equivalence relation we are now ready to construct the Brauer group.

**Definition:** We denote by $[A]$ the equivalence class of the Azumaya $R$-algebra $A$ under the equivalence relation $\sim$. We define the **Brauer group** of a commutative ring $R$, denoted by $\boldsymbol{Br(R)}$, as the set of equivalence classes of Azumaya $R$-algebras, with the tensor product as the group operation and with $[R]$ acting as the identity element.

Recall from Proposition 8.3 that $End_R(P)$ is an Azumaya algebra for any faithfully projective $R$-module $P$. Also note that $[End_R(P)] = [R] = 1 \in Br(R)$ by definition of $\sim$.

Collecting the above observations together with the propositions of the previous sections, we now show that $Br(R)$ is indeed a group.

**Theorem 8.5** *$Br(R)$ with multiplication defined by $[A] \bullet [B] = [A \otimes B]$ is an abelian group.*

**Proof:** It is easy to check that if $A \sim A'$ and $B \sim B'$ for Azumaya algebras $A, A', B, B'$ then $A \otimes B \sim A' \otimes B'$ (Exercise 5). Since it is also true that $A \otimes B$ is an Azumaya algebra if both $A$ and $B$ are (Proposition 8.4), we see that $\otimes$ gives a well-defined multiplication on the set of equivalence classes of Azumaya $R$-algebras. This multiplication is clearly associative and commutative. $[R] = [End_R(P)]$ for $P$ faithfully projective acts as identity element by definition of $\sim$. Finally, if $A$ is Azumaya then so is $A^\circ$, and

$$[A] \bullet [A^\circ] = [A \otimes A^\circ] = [End_R(A)] = 1 \in Br(R)$$

so that $[A^\circ]$ is the inverse of $[A]$ in $Br(R)$. □

## Homomorphisms and Functoriality

Just as we saw in the case of fields, homomorphisms between Brauer groups can be just as important as the Brauer groups themselves. We shall now prove that $Br()$ is a (covariant) functor from the category of commutative rings and ring homomorphisms to the category of abelian groups and group homomorphisms. For those not familiar with these terms from category theory, this can be phrased as saying that to each commutative ring $R$ there is an associated group $Br(R)$, and to each homomorphism $f : R \longrightarrow S$ of commutative rings there is an associated homomorphism $Br(f) : Br(R) \longrightarrow Br(S)$ of abelian groups, so that

1. If $g : S \longrightarrow T$ is another homomorphism of commutative rings then $Br(g \circ f) = Br(g) \circ Br(f)$, and
2. If $f : R \longrightarrow R$ is the identity homomorphism then $Br(f) : Br(R) \longrightarrow Br(R)$ is the identity homomorphism.

So suppose that $f : R \longrightarrow S$ is a homomorphism of commutative rings. Then $S$ becomes a commutative $R$-algebra via

$$r \cdot s = f(r)s.$$

If $A$ is an $R$-algebra then $A \otimes_R S$ is an $S$-algebra. An obvious candidate for $Br(f)$ is

$$Br(f) : Br(R) \longrightarrow Br(S)$$

$$[A] \longmapsto [A \otimes_R S]$$

Before proving that $Br(f)$ is well-defined we shall need the following two lemmas, which relate certain tensor products over $R$ to others over $S$.

**Lemma 8.6** *If $A$ and $B$ are $R$-algebras and if $S$ is a commutative $R$-algebra then $(A \otimes_R S) \otimes_S (B \otimes_R S) \approx (A \otimes_R B) \otimes_R S$ as $S$-algebras.*

**Proof:** We leave as an exercise (Exercise 7) to the reader the fact that the map defined by

$$(A \otimes_R S) \otimes_S (B \otimes_R S) \longrightarrow (A \otimes_R B) \otimes_R S$$

$$(a \otimes s) \otimes (b \otimes s') \longmapsto (a \otimes b) \otimes ss'$$

extended linearly is an isomorphism. □

**Lemma 8.7** *If $A$ is a faithfully projective $R$-algebra and $S$ is a commutative $R$-algebra then $End_R(A) \otimes_R S \approx End_S(A \otimes_R S)$.*

**Proof:**

We define a homomorphism $\phi : End_R(A) \otimes_R S \longrightarrow End_S(A \otimes_R S)$ by

$$\phi(f \otimes s)(a \otimes s') = f(a) \otimes ss'$$

extended linearly, where $f \in End_R(A), a \in A$, and $s, s' \in S$. As $A$ is a faithfully projective $R$-module, there exists an $R$-module $B$ with $A \oplus B \approx R^n$. We then have the following commutative diagram :

$$\begin{array}{ccc} End_R(A) \otimes_R S & \xrightarrow{\quad \phi \quad} & End_S(A \otimes_R S) \\ \downarrow \uparrow & & \downarrow \uparrow \\ End_R(R^n) \otimes_R S & \xrightarrow{\quad \phi' \quad} & End_S(R^n \otimes_R S) \end{array}$$

where the vertical maps are induced by the inclusion $A \hookrightarrow A \oplus B$ as discussed on page 187, and $\phi'$ is defined by

$$\phi'(f \otimes s)(v \otimes s') = f(v) \otimes ss'$$

extended linearly, where $f \in End_R(R^n), v \in R^n$, and $s, s' \in S$. Since the above diagram (including the splitting maps) commutes, it suffices to show that $\phi'$ is an isomorphism.

Let $\{e_1, \ldots, e_n\}$ be an $R$-algebra basis for $A \oplus B \approx R^n$, so that $\{e_i \otimes 1\}$ is an $S$-algebra basis for $(A \oplus B) \otimes_R S \approx R^n \otimes_R S$. Let $E_{ij} \in End_R(R^n)$ be defined, as always, by

$$E_{ij}(e_k) = \delta_{ik}e_j, \quad 1 \leq i, j \leq n$$

so that $\{E_{ij}\}$ is an $R$-algebra basis for $End_R(R^n)$. To show that $\phi'$ is onto, let $h \in End_S(R^n \otimes S)$ be given. Then $h(e_i \otimes 1) = \sum_j e_j \otimes s_{ij}$ for some $s_{ij} \in S$. For each $i$,

$$\begin{aligned}\phi'(\textstyle\sum_{i,j} E_{ij} \otimes s_{ij})(e_i \otimes 1) &= \textstyle\sum_{i,j} E_{ij}(e_i) \otimes s_{ij} \\ &= \textstyle\sum_j r_j \otimes s_{ij} \\ &= h(e_i \otimes 1).\end{aligned}$$

Since $\{e_i \otimes 1\}$ forms an $S$-algebra basis for $R^n \otimes S$ and since elements of $End_S(R^n \otimes S)$ are determined uniquely by their value on a basis, we see that $\phi'$ is onto.

To show that $\phi'$ is one-to-one, first note that any element $h \in End_R(R^n) \otimes S$ can be written uniquely as

$$h = \sum_{i,j} E_{ij} \otimes s_{ij}$$

with $s_{ij} \in S$. Then $\phi'(h)(e_i \otimes 1) = \sum_j r_j \otimes s_{ij}$. If $\phi'(h) = 0$, then $\phi'(h)(e_i \otimes 1) = 0$ for each $i$, so that $\sum_j s_{ij}(e_j \otimes 1) = \sum_j r_j \otimes s_{ij} = 0$. Since $\{e_j \otimes 1\}$ forms a basis for $R^n \otimes S$, this implies that $s_{ij} = 0$ for each $j$ and for each $i$. Hence $h = 0$ and we are done. □

To show that $Br(f)$ is well-defined we must first show that the operation of tensoring with $S$ (over $R$) takes Azumaya $R$-algebras to Azumaya $S$-algebras.

**Lemma 8.8** *If $A$ is an Azumaya $R$-algebra and $S$ is a commutative $R$-algebra then $A \otimes_R S$ is an Azumaya $S$-algebra.*

**Proof:** We leave as an exercise (Exercise 4) the fact that if $A$ is a faithfully projective $R$-algebra and $S$ is a commutative $R$-algebra then $A \otimes_R S$ is a faithfully projective $S$-algebra. To prove that condition (2) in the definition of Azumaya algebra holds, we note that the following diagram is commutative:

$$\begin{array}{ccc}(A \otimes_R S) \otimes_S (A \otimes_R S)^\circ & \xrightarrow{\ \Psi_{A \otimes S}\ } & End_R(A \otimes_R S) \\ \approx \big\downarrow & & \big\uparrow \phi \ \approx \\ (A \otimes_R A^\circ) \otimes_R S & \xrightarrow[\approx]{\ \Psi_A \otimes 1_S\ } & End_R(A) \otimes S\end{array}$$

where $\psi_A : A \otimes_R A^\circ \longrightarrow End_R(A)$ is the isomorphism coming from the fact that $A$ is an Azumaya $R$-algebra, $\phi$ is the isomorphism coming from Lemma 8.7, and the left-side vertical isomorphism comes from Lemma 8.6. Hence $\psi_{A\otimes S}$ is an isomorphism. □

With these lemmas it is now possible to prove that $Br()$ is a functor.

**Theorem 8.9** *$Br()$ is a functor from the category of commutative rings and ring homomorphisms to the category of abelian groups and group homomorphisms.*

**Proof:** Let $f : R \longrightarrow S$ be a homomorphism of commutative rings. By Lemma 8.8 we have that the operation of tensoring with $S$ (over $R$) takes Azumaya $R$-algebras to Azumaya $S$-algebras. To prove that $Br(f)$ is well-defined we must check that $Br(f)$ preserves the equivalence relation $\sim$. So suppose that $A$ and $B$ are $R$-algebras with $A \sim B$, say $A \otimes_R End_R(P) \approx B \otimes_R End_R(Q)$ for some faithfully projective $R$-modules $P$ and $Q$. Tensoring both sides by $\otimes_R S$ gives

$$(A \otimes_R End_R(P)) \otimes_R S \approx (B \otimes_R End_R(Q)) \otimes_R S$$

and by an application of Lemma 8.6 this gives

$$(A \otimes_R S) \otimes_S (End_R(P) \otimes_R S) \approx (B \otimes_R S) \otimes_S (End_R(Q) \otimes_R S).$$

Since, by Lemma 8.7, $End_R(P) \otimes_R S \approx End_S(P \otimes_R S)$ and $End_R(Q) \otimes_R S \approx End_S(Q \otimes_R S)$, it follows that

$$(A \otimes_R S) \otimes_S End_S(P \otimes_R S) \approx (B \otimes_R S) \otimes_S End_S(Q \otimes_R S).$$

Since $P \otimes_R S$ and $Q \otimes_R S$ are faithfully projective $S$-modules, this says that $(A \otimes_R S) \sim (B \otimes_R S)$ as $S$-algebras, so that $Br(f) : Br(R) \longrightarrow Br(S)$ is well-defined. Furthermore, for Azumaya $R$-algebras $A$ and $B$ we have

$$\begin{aligned} Br(f)([A] \bullet [B]) &= Br(f)([A \otimes_R B]) \\ &= [(A \otimes_R B) \otimes_R S] \\ &= [(A \otimes_R S) \otimes_S (B \otimes_R S)] \quad \text{by Lemma 8.6} \\ &= [A \otimes_R S] \bullet [B \otimes_R S] \\ &= Br(f)([A]) \bullet Br(f)([B]) \end{aligned}$$

so that $Br(f)$ is a group homomorphism. It is now trivial to verify that $Br(f)$ is a functor. □

The fact that $Br()$ is a functor may be used to relate Brauer groups of various rings and fields. We list a few examples, followed by references for their proofs.

**Examples:**

1. If $R$ is the ring of algebraic integers in a (finite) algebraic number field, then $Br(R)$ is a direct product of cyclic groups of order 2. A special case of this theorem implies that $Br(\mathbf{Z}) = 0$.

2. If $I$ is an ideal in the commutative ring $R$, then the canonical homomorphism $R \longrightarrow R/I$ induces a homomorphism of Brauer groups $Br(R) \longrightarrow Br(R/I)$. This homomorphism is an isomorphism whenever $I$ is a nilpotent ideal, or when $R$ is a complete local ring with maximal ideal $I$.

3. If $R$ is an integral domain with field of fractions $k$, then the homomorphism $Br(R) \longrightarrow Br(k)$ induced by the inclusion $R \hookrightarrow k$ is often one-to-one. This happens, for example, when $R$ is a regular domain. The homomorphism from $Br(R)$ to $Br(k)$ is rarely onto; for example $Br(\mathbf{Z}) = 0$ but $Br(\mathbf{Q}) \neq 0$.

4. If $R$ is any ring we have homomorphisms

$$R \xrightarrow{i} R[x] \xrightarrow{j} R$$

where $R[x]$ denotes the ring of polynomials in one variable over $R$, $i$ denotes the inclusion homomorphism, and $j : R[x] \longrightarrow R$ is the $R$-homomorphism determined by $j(x) = 0$. Note that $j \circ i$ is the identity. If $R$ is commutative, this sequence induces homomorphisms

$$Br(R) \xrightarrow{Br(i)} Br(R[x]) \xrightarrow{Br(j)} Br(R)$$

with $Br(j) \circ Br(i)$ the identity by functoriality. In particular, $Br(i)$ is injective, $Br(j)$ is surjective, and $Br(R[x])$ is the direct sum of $Br(R)$ and $kernel(Br(j))$. When $R$ is a field, $Br(i)$ is an isomorphism if and only if $R$ is perfect.

These and other examples are discussed in D. Zelinsky's survey article "Brauer Groups". Their proofs are beyond the scope of this book; the proof of Example 1 can be found in Grothendieck, "Le Groupe de Brauer, I, II, III", while the proofs of Examples 2,3, and 4 can be found in Auslander and Goldman, "The Brauer Group of a Commutative Ring".

# Exercises

1. An algebra $A$ over a commutative ring $R$ is called **central** if $Z(A) = R$. The goal of this exercise is to prove that Azumaya algebras are central.

(a) Prove that any idempotent finitely generated ideal of a commutative ring $R$ is principal.

(b) If $M$ is any $R$-module, let

$$\mathcal{T}_R(M) = \{\sum_i f_i(m_i) : f_i \in Hom_R(M, R), m_i \in M\}$$

Then $\mathcal{T}_R(M)$ is a two-sided ideal of $R$, called the **trace ideal** of $M$. Show that the trace ideal of any faithfully projective $R$-module is all of $R$.

(c) Prove that if $A$ is a faithfully projective $R$-algebra, and if we identify $R$ with the image of the algebra-structure map $R \longrightarrow A$, then $R$ is an $R$-module direct summand of $A$. [Hint : Apply part (b) to $1 \in R$.]

(d) Suppose that $A$ is an $R$-algebra which is faithfully projective as an $R$-module and faithful as an $A^e$-module. Prove that $A$ is central. Conclude that Azumaya algebras are central. [Hint : Let $A = R \oplus P$ be the splitting given by part (c). Since $R$ is central in $A$, it will suffice to show that any nonzero element of $P$ is not central. Prove that, for any $p \in P$, $1 \otimes p$ and $p \otimes 1$ are distinct in $A^e$. Now show that this implies that $p$ is not central.]

2. Generalize Proposition 8.1 as follows : Let $R$ be a commutative ring. Show that the natural map

$$Hom(R^m, R^{m'}) \otimes Hom(R^n, R^{n'}) \longrightarrow Hom(R^m \otimes R^n, R^{m'} \otimes R^{n'})$$

is an isomporphism for any positive integers $m, n, m', n'$.

3. (a) Show that if $M$ and $N$ are finitely generated $R$-modules, then $M \otimes N$ is a finitely generated $R$-module.

(b) Show that if $M$ and $N$ are projective $R$-modules then $M \otimes N$ is a projective $R$-module.

(c) Give an example to show that the tensor product of two faithful $R$-modules is not necessarily faithful. Show that if $M$ and $N$ are faithfully projective $R$-modules then $M \otimes N$ is a faithfully projective $R$-module.

4. Let $S$ be a commutative $R$-algebra.

(a) Show that if $A$ is a finitely generated $R$-module then $A \otimes_R S$ is a finitely generated $S$-module.

(b) Show that if $A$ is a projective $R$-module then $A \otimes_R S$ is a projective $S$-module.

(c) Give an example to show that, even if $A$ is a faithful $R$-module, $A \otimes_R S$ may not be a faithful $S$-module. [Hint: Look at the ring of continuous, real-valued functions on the unit interval, and the ideal of functions which are zero in some neighborhood of 0.] Show that if $A$ is a faithfully projective $R$-module then $A \otimes_R S$ is a faithfully projective $S$-module.

5. Prove that if $A \sim A'$ and $B \sim B'$ for Azumaya algebras $A, A', B, B'$ then $A \otimes B \sim A' \otimes B'$.

6. (a) Prove that $[A] = [R] = 1$ in $Br(R)$ if and only if $A \approx End_R(P)$ for some faithfully projective $R$-module $P$.

   (b) Prove that $[A] = [B]$ in $Br(R)$ if and only if $A \otimes_R B^\circ \approx End_R(P)$ for some faithfully projective $R$-module $P$.

7. Prove Lemma 8.6; that is, if $A$ is an $R$-algebra and $S$ is a commutative $R$-algebra then the map defined by

$$(A \otimes_R S) \otimes_S (B \otimes_R S) \longrightarrow (A \otimes_R B) \otimes_R S$$

$$(a \otimes s) \otimes (b \otimes s') \longmapsto (a \otimes b) \otimes ss'$$

   extended linearly is an isomorphism.

8. Verify that $Br()$ is a functor.

9. Show that there is no subring $A$ of the real quaternions $\mathbf{H}$ such that: $A$ is free of rank 4 over $\mathbf{Z}$; $A \otimes_{\mathbf{Z}} \mathbf{R} = \mathbf{H}$ (i.e., $A$ contains a basis for $\mathbf{H}$ over $\mathbf{R}$); and $A$ is an Azumaya algebra over $\mathbf{Z}$. In particular, the $\mathbf{Z}$-algebra of "integer quaternions", i.e. the set of real quaternions with integer coordinates, is not an Azumaya algebra over $\mathbf{Z}$. [Hint: Tensor with $\mathbf{Z}/2\mathbf{Z}$ and use exercise 1.]

10. (a) Let $R$ be a commutative ring in which 2 is invertible. Define the quaternions $Q$ over $R$ as follows : $Q$ is a free $R$-module with basis $1, i, j, k$ and multiplication satisfying $i^2 = j^2 = k^2 = -1, ij = k = -ji$. Show that $Q$ is an Azumaya $R$-algebra. What can you say about the order of $[Q]$ in $Br(R)$?

    (b) Let $R$ be as in part (a), and let $a$ and $b$ be units in $R$. define the generalized quaternion algebra $\left(\frac{a, b}{R}\right)$ to be the free $R$-algebra with basis $\{1, i, j, k\}$ satisfying $i^2 = a, j^2 = b, ij = -ji = k$. Show that $\left(\frac{a, b}{R}\right)$ is an Azumaya algebra.

# Part III

# Supplementary Exercises

1. Let $k$ be a field, and let $R$ be a $k$-subalgebra of $\mathcal{M}_n(k)$ with the property that every simple $R$-module is a $k$-space of dimension one. Show that there is an invertible matrix $u \in \mathcal{M}_n(k)$ such that all elements of $uRu^{-1}$ are upper triangular matrices. [Hint: Look at a composition series of $R$ as a left $R$-module.]

2. (a) Let $A$ be a finite-dimensional algebra over a field. Show that if $a \in A$, then either a has a two-sided inverse in $A$ or there exists $b \neq 0$ in $A$ such that $ab = 0 = ba$; in particular, if $A$ is an integral domain, then it is a division ring. [Hint: Use the "minimal polynomial" of $a$.]

   (b) Give an example of a ring $R$ and an element $a \in R$ that has a left inverse but no right inverse.

### The Ore Condition and the Construction of Division Rings of Fractions

One common way of constructing fields is to take the field of fractions of a commutative integral domain, a process exactly like that of constructing the field of rational numbers from the ring of integers. There is an analogous process in the noncommutative case, whereby one may construct the "division ring of fractions" from a (not necessarily commutative) integral domain. This construction does not work for every integral domain, but in the 1940's, O. Ore gave a precise condition on an integral domain which tells when the division ring of fractions may be constructed. This provides us with many more examples of division rings, one of the basic objects of study in this book.

3. Let us begin with the easier case of constructing the field of fractions of a commutative integral domain $R$. Let $S = \{(a, b) : a, b \in R, b \neq 0\}$, and define an equivalence relation $\sim$ on $S$ by setting $(a, b) \sim (a', b')$ if $ab' = a'b$. Denote the equivalence class of $(a, b)$ by $a/b$. Show that setting

$$a/b + c/d = (ad + bc)/bd$$

and

$$a/b \cdot c/d = ac/bd$$

is well-defined and makes the set of equivalence classes in $S$ into a field containing $R$. Show that this field is the smallest field containing $R$.

4. (a) Now let us generalize the construction of the field of fractions to the case of an integral domain $R$ which is not necessarily commutative. $R$ is said to satisfy the **right Ore condition** if for all $a, b \in R$, both nonzero, there exist $a', b' \in R$ (both nonzero) so

that $aa' = bb'$; that is, $a$ and $b$ have a common right multiple. Let $S = \{(a,b) : a,b \in R, b \neq 0\}$, and define an equivalence relation $\sim$ on $S$ by setting $(a,b) \sim (c,d)$ if $ab' = cd'$, where $bb' = dd'$ via the Ore condition. Show that this is an equivalence relation. Let $D$ be the set of equivalence classes in $S$. Define an addition by

$$a/b + c/d = (ab' + cd')/bb'$$

where $bb' = dd'$ via the Ore condition, and define a multiplication by

$$a/b \cdot c/d = ab'/dc'$$

where $bb' = cc'$ via the Ore condition. Show that these operations are well-defined, and that they make $D$ into a division algebra containing $R$.

(b) Prove a universal mapping property for $R$ with respect to $D$. Conversely to the above, show that any ring which has a division ring of fractions must satisfy the right Ore condition.

(c) Give the definition of left Ore condition, and mentally go through this exercise again for rings satisfying the left Ore condition.

5. Let $D$ be a division algebra.

(a) Show that $D[x]$ satisfies both the right and left Ore condition. In fact, show that a ring $R$ satisfies the (right) Ore condition if and only if the polynomial ring $R[x]$ does.

(b) Let $F$ be a field, and let $F\{x,y\}$ be the **free algebra** on $x$ and $y$. This algebra is similar to the polynomial algebra $F[x,y]$, except that $x$ and $y$ do not commute in $F\{x,y\}$. Show that $F\{x,y\}$ does not satisfy either Ore condition.

(c) Let $\sigma$ be an automorphism of $D$, and let $D[x;\sigma]$ denote the **twisted polynomial ring** of $D$ twisted by $\sigma$. This ring is defined to be the polynomial ring $D[x]$ with multiplication defined by

$$xa = \sigma(a)x,$$

so for example

$$(ax^m)(bx^n) = a\sigma^m(b)x^{m+n}.$$

Show that $D[x;\sigma]$ satisfies both the right and left Ore conditions.

(d) Now let $\sigma$ be any endomorphism of $D$. Let $\delta : D \longrightarrow D$ be a **$\sigma$-derivation** , which means that

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b \quad \text{for } a,b \in D.$$

Denote by $D[x;\sigma,\delta]$ the polynomial ring $D[x]$ with multiplication defined by

$$xa = \sigma(a)x + \delta(a).$$

This generalizes the concept of twisted polynomial ring. Show that the following are equivalent:

(1) $\sigma$ is onto.

(2) $D[x;\sigma,\delta]$ satisfies the right Ore condition.

(3) Every right ideal of $D[x;\sigma,\delta]$ is principal.

### More on Injective Modules

6. Recall that $\mathbf{Z}$-modules are precisely the abelian groups, and (Chapter 1, Exercise 36) injective $\mathbf{Z}$-modules are precisely the divisible abelian groups. Prove that every abelian group can be embedded in a divisible group; in other words, every $\mathbf{Z}$-module can be embedded in an injective $\mathbf{Z}$-module. [Hint: Do it first for free abelian groups.]

7. The goal of this exercise is to classify all injective $\mathbf{Z}$-modules (i.e. all divisible abelian groups).

   (a) Let $T(G)$ denote the torsion subgroup of $G$; that is, $T(G)$ is the set of elements of $G$ which have finite order. Show that $G/T(G)$ is torsion-free. Show that if $G$ is divisible, then $G \approx T(G) \oplus (G/T(G))$, and both $T(G)$ and $G/T(G)$ are divisible.

   (b) Show that any torsion-free divisible group is a direct sum of copies of $\mathbf{Q}$.

   (c) A group $G$ is called a **$p$-primary** ($p$ a prime) if every element of $G$ has order some power of $p$. Let $G$ and $H$ be divisible $p$-primary groups, and let $G_p$ (resp. $H_p$) denote the subgroup of $G$ (resp. $H$) consisting of elements annihilated by $p$. Prove that $G \approx H$ if and only if $G_p \approx H_p$. [Hint: One direction is clear; for the other, think of the isomorphism $\phi : G_p \longrightarrow H_p$ as a map $\phi : G_p \longrightarrow H$. Now use the extension property of injective modules (Exercise 35 of Chapter 1) to find a map from $G$ to $H$. Show that this map is an isomorphism.]

   (d) Recall that $\mathbf{Z}_{p^\infty}$ denotes the submodule of the $\mathbf{Z}$-module $\mathbf{Q}/\mathbf{Z}$ consisting of elements which are annihilated by some power of $p$. Prove that every divisible group $G$ (i.e., every injective $\mathbf{Z}$-module) is isomorphic to a direct sum of copies of $\mathbf{Q}$ and $\mathbf{Z}_{p^\infty}$ (for various primes $p$). [Hint: The number of copies of $\mathbf{Z}_{p^\infty}$ for a given prime $p$ is equal to the dimension of $G_p$ as a vector space over $\mathbf{Z}/p\mathbf{Z}$.]

(e) If $G$ is a divisible group, note that $G/T(G)$ is a vector space over $\mathbf{Q}$, and $T(G)_p$ is a vector space over $\mathbf{Z}/p\mathbf{Z}$. Prove that, if $G$ and $H$ are divisible groups, then $G \approx H$ if and only if

(i) $G/T(G)$ and $H/T(H)$ have the same dimension; and

(ii) For each prime $p$, $T(G)_p$ and $T(H)_p$ have the same dimension.

8. This exercise gives a method for constructing injective modules over an arbitrary ring $R$. Let $R$ be a ring and let $A$ be an abelian group.

(a) Show that $Hom_{\mathbf{Z}}(R, A)$ becomes a left $R$-module via $(rf)(s) = f(sr)$. Similarly, it becomes a right $R$-module via $(fr)(s) = f(rs)$.

(b) If $Q$ is an injective $\mathbf{Z}$-module (i.e. a divisible abelian group), show that $Hom_{\mathbf{Z}}(R, Q)$ is an injective $R$-module. Do this by applying Exercise 35 of Chapter 1: Given a left ideal $L$ of $R$ and a homomorphism $f : L \longrightarrow Hom_{\mathbf{Z}}(R, Q)$, consider the function

$$g : L \longrightarrow Q$$

defined by

$$g(x) = f(x)(1).$$

This is a $\mathbf{Z}$-homomorphism and by the $\mathbf{Z}$-injectivity of $Q$ extends to a $\mathbf{Z}$-homomorphism $g' : R \longrightarrow Q$. Let

$$f' : R \longrightarrow Hom_{\mathbf{Z}}(R, Q)$$

be defined by

$$f'(x)(y) = g'(yx).$$

Show that $f'$ is an $R$-homomorphism which extends $f$.

(c) Show that every $R$-module can be embedded in an injective $R$-module. [Hint: Apply $Hom_{\mathbf{Z}}(R,\ )$ to exercise 6 and note that for an $R$-module $M$, we have $M \approx Hom_R(R, M) \subseteq Hom_{\mathbf{Z}}(R, M)$. Note that the $R$-module structure here for $Hom_R(R, M)$ is given as above; this is not the usual way, but fortunately it doesn't make any difference here.]

**Remark:** These results are used in homological algebra to construct injective resolutions of modules; that is, we can obtain, for each $M$, an exact sequence of the form

$$0 \longrightarrow M \longrightarrow Q_1 \longrightarrow Q_2 \longrightarrow Q_3 \longrightarrow \cdots$$

with each $Q_i$ injective.

9. Let $R$ be a commutative Noetherian ring, $Q$ be an injective $R$-module, and $I$ be an ideal of $R$. Show that the set of elements $x \in Q$ such that $I^n x = 0$ for some $n$ (depending on x) is an injective $R$-module. [Hint : Use Chapter 0, Exercise 35.]

### The Big Ring: A Counterexample to Everything

10. Let $V$ be a vector space of countably infinite dimension over a field $k$. Let $I$ be the set of finite rank operators; i.e., those elements of $End_k(V)$ whose image is finite dimensional. Show that $I$ forms a two-sided in $End_k(V)$; hence $End_k(V)$ is not simple, in contrast to the fact that endomorphism rings of finite dimensional vector spaces are simple.

11. With the notation as above, let $R = Endk(V)/I$. We shall call the ring $R$ **the Big Ring** (certain people have refered to this ring as the **Mother of all Rings**). The Big Ring has several interesting properties, and provides, for many theorems, an example to show that the theorem does not hold if the assumption of finite-dimensionality is dropped. The Big Ring also provides certain counterexamples in algebraic $K$-theory. Prove the following facts about the Big Ring $R$:

    (a) The Big Ring is a simple ring which is not semisimple.

    (b) $R \approx R \oplus R$ as $R$-modules (but not as rings, of course).

    (c) $R \approx \mathcal{M}_2(R)$.

    (d) Let $\phi : \mathcal{M}_2(R) \longrightarrow R$ be an isomorphism, and let $diag : R \longrightarrow \mathcal{M}_2(R)$ denote the map which takes $r \in R$ to the $2 \times 2$ diagonal matrix each of whose nonzero entries is $r$. Let $\Delta : R \longrightarrow R$ be the composition $\Delta = \phi \circ diag$. Let $S$ be the direct limit of the sequence

    $$R \xrightarrow{\Delta} R \xrightarrow{\Delta} R \xrightarrow{\Delta} R \xrightarrow{\Delta} \cdots.$$

    Show that $S$ is actually isomorphic to a subalgebra of $R$. Is $S$ isomorphic to $R$?

    (e) Use parts (c) and (d) of this exercise to give counterexamples to both parts of the Skolem-Noether Theorem.

### Other Examples of How Skolem-Noether Can Fail

The examples in this section will show how both parts of the Skolem-Noether may fail, even in the case of central division algebras.

12. Let $D_1 \subseteq D_2 \subseteq \cdots$ be a (not necessarily finite) increasing sequence of division rings. Show that the union $\bigcup_i D_i$ is a division ring.

13. (a) Let $F$ be a field with $char(F) \neq 2$, and let $K = F(x_1, y_1, x_2, y_2, \ldots)$, where each $x_i$ and each $y_i$ is an indeterminate over $F$. The field $K$ is called a **function field** in infinitely many variables. Let $\left(\frac{x,y}{K}\right)$ denote a generalized quaternion algebra over $K$ (for information on these algebras, see the exercises of Chapter 4). Show that

$$\left(\frac{x_1, y_1}{K}\right) \otimes_K \left(\frac{x_2, y_2}{K}\right) \otimes_K \cdots \otimes_K \left(\frac{x_i, y_i}{K}\right)$$

is a division algebra for each $i$.

(b) Use the division algebras from part (a) to come up with an example which shows that neither part of the Skolem-Noether Theorem necessarily holds if the subalgebras are not finite dimensional.

14. (a) Let $D_1, D_2, \ldots$ be an infinite sequence of division algebras of relatively prime degree over a field $k$. Show that

$$D_1 \otimes_k D_2 \otimes_k \cdots \otimes_k D_i$$

is a division algebra for each $i$ (cf. Chapter 4, Exercise 4.18).

(b) Use the division algebras from part (a) to come up with an example which shows that neither part of the Skolem-Noether Theorem necessarily holds if the subalgebras are not finite dimensional.

### Maximal Commutative Subalgebras

15. Let $A$ be a central simple algebra over a field $k$, and let $K$ and $L$ be commutative subalgebras of $A$. Prove the following facts:

(a) $A$ is a faithful $K \otimes_k L$-module.

(b) The $K \otimes_k L$-module $A$ is projective and has a summand isomorphic to $K \otimes_k L$.

(c) $[K : k][L : k] \leq [A : k]$; in particular $[A : k] \geq [K : k]^2$.

16. Derive the following corollary to Exercise 15: Let $K, L \subseteq A$ as in Exercise 15 with both $K$ and $L$ semisimple. Then the following are equivalent:

(a) $K$ and $L$ are maximal commutative subalgebras of $A$.

(b) $A \approx K \otimes_k L$ as $K \otimes_K L$-modules.

(c) $[A : k] = [K : k][L : k]$

17. Let $A$ be a central simple $k$-algebra with commutative semisimple subalgebra $K$. Prove that the following are equivalent:

(a) $K$ is a maximal commutative subalgebra of $A$.

(b) $A \approx K \otimes_k K$ as $K \otimes_k K$-modules.

(c) $[A : k] = [K : k]^2$.

18. Prove the following generalization of Theorem 4.4: If $A$ is a central simple k-algebra, and if $K$ is a maximal commutative semisimple subalgebra of $A$, then $K$ splits $A$. [Hint: Use the Double Centralizer Theorem.]

19. Let $A$ be a central simple $k$-algebra with $[A : k] = n^2$. Let $\alpha \in A$, and let $f$ be the minimal polynomial of $\alpha$ over $k$. Assume that $deg(f)f = n$, $f$ is separable, and $f$ has a root in $k$. Prove that $A \approx \mathcal{M}_n(k)$.

### Primitive Rings and Density

20. Let $I$ be a two-sided ideal in a dense ring of linear transformations of a vector space $V$ over a division ring $D$. Prove that $I$ itself is dense; that is, show that if $\{v_1, \ldots, v_n\}$ is a linearly independent set of vectors in $V$, and if $\{w_1, \ldots, w_n\}$ is an arbitrary set of vectors in $V$, then there exists $\phi \in I$ with $\phi(v_i) = w_i$ for $1 \leq i \leq n$.

21. Let $R$ be a ring with $J(R) = 0$ such that for all $a, b, c \in R$,

$$a(bc - cb) = (bc - cb)a.$$

Show that $R$ is a subdirect product of division rings. [Hint: First assume that $R$ is (left) primitive and that $[V : D] > 1$, where $V$ is a faithful simple $R$-module with endomorphism ring $D$. Choose $a, b, c$ like matrices and get $[V : D] = 1$.

22. Prove that if a (left) primitive ring $R$ contains a finite nonzero left ideal then $R$ is finite.

23. Let $F$ be a field of characteristic 0 and let $F\{x, y\}$ denote the free algebra over $F$ generated by $x$ and $y$. Let $I$ denote the ideal of $F\{x, y\}$ generated by $xy - yx - x$. Show that $F\{x, y\}/I$ is primitive.

24. Let $R = F[t_1, \ldots, t_n]$ be the polynomial ring in $n$ indeterminates over a field $F$.

(a) Show that for each $i$ with $1 \leq i \leq n$ there is a unique derivation $d_i$ of $R$ with $d_i(t_j) = \delta_{ij}$.

(b) As usual, for $r \in R$ let $T_r$ denote be the map $T_r(s) = rs$. Show that if $D$ is any derivation of $R$, and if $r \in R$, then $T_r \circ D$ is also a derivation of $R$.

(c) Show that every derivation of $R$ is of the form

$$\sum_{i=1}^{n} T_{r_i} d_i$$

where the $d_i$ are as in part (a) and $r_i \in R$. Conversely, all such sums are derivations of $R$.

(d) Let $S$ be the ring of endomorphisms of the additive group of $R$ generated by the derivations and the $T_r$'s, $r \in R$. Assuming that $F$ has characteristic 0, show that $S$ is simple, hence primitive.

25. Let $F$ be a field of characteristic 0, and let $F\{x_1, \ldots x_n, y_1, \ldots, y_n\}$ be the free algebra on $2n$ indeterminates. Suppose that $I$ is the ideal in $F\{x_1, \ldots x_n, y_1, \ldots, y_n\}$ generated by elements of the form

$$[x_i, x_j],\ [y_i, y_j],\ [y_i, x_j] - \delta_{ij} \quad 1 \le i, j \le n.$$

Let $W_n = F\{x_1, \ldots x_n, y_1, \ldots, y_n\}/I$. $W_n$ is called the **Weyl algebra**. Let $R$ and $S$ be as in exercise 24. Let

$$\phi : F\{x_1, \ldots x_n, y_1, \ldots, y_n\} \longrightarrow S$$

$$x_i \longmapsto T_{t_i}$$

$$y_i \longmapsto d_i$$

for $1 \le i \le n$. Show that $\phi$ is surjective and has kernel $I$. Conclude that the Weyl algebra $W_n$ is primitive.

26. (a) Show that the Weyl algebra $W_1$ is simple.

(b) Show more generally that the Weyl algebra $W_n$ is simple.

27. This exercise constructs a division ring $R$ which is artinian, yet has the property that for every positive integer $n$, there exists a subring $R_n$ of $R$ which maps homomorphically onto $\mathcal{M}_n(D)$, where $D = End_R(M)$, $M$ a faithful simple $R$-module (compare with Theorem 5.4 and the discussion that follows).

(a) Let $L_0$ be a field containing all $n$th roots of unity (e.g., the complex numbers). Let $L = L_0(z)$, $z$ an indeterminate. Let $L_n = L_0(\sqrt[n]{z})$. Then The Galois group $Gal(L_n/L)$ is the cyclic group of order $n$, say generated by the automorphism $\sigma_n$. Let $R_n = L_n[x_n; \sigma_n]$ be the twisted polynomial ring over the indeterminate $x_n$ with twist $\sigma_n$ (recall that $R_n$ is simply the polynomial ring $L_n[x_n]$ with multiplication defined by $x_n a = \sigma_n(a) x_n$). Define a map

$$R_n \longrightarrow \mathcal{M}_n(L)$$
$$x_n \longmapsto C(y^n - z)$$

where $C = C(y^n - z)$ denotes the companion matrix of the polynomial $y^n - z$ over $L$. Show that this map is surjective. [Hint: Let $\zeta$ be a primitive $n$th root of unity. The matrix

$$S = \begin{bmatrix} 1 & & & 0 \\ & \zeta & & \\ & & \ddots & \\ 0 & & & \zeta^{n-1} \end{bmatrix}$$

has the property that $SCS^{-1} = \zeta C$, and is an explicit matrix that conjugates like the Skolem-Noether theorem says.]

(b) Use the rings $R_p$ as $p$ runs over all primes to form a ring $R$ which satisfies the Ore condition, and let $\Delta$ be the division ring of fractions of $R$ (cf. exercises 4 and 5). Show that $\Delta$ is the division ring we are looking for.

### von Neumann Regular Rings

28. Prove that the following three conditions on a ring $R$ are equivalent:

(i) Every principal left ideal of $R$ is generated by an idempotent.

(ii) For any $a \in R$, there exists $b \in R$ with $aba = a$.

(iii) Every principal right ideal of $R$ is generated by an idempotent.

A ring satisfying these conditions is called **von Neumann regular**, or simply **regular**. Such rings were introduced by (you guessed it) von Neumann in his work on so-called "continuous geometries" in the mid 1930's.

29. Show that a regular ring is a division ring if and only if its only idempotents are 0 and 1.

30. Show that the following rings are regular:

(a) Division rings.

(b) Products of regular rings.

(c) $End_D(V)$, where $V$ is a (not necessarily finite dimensional) vector space over the division ring $D$.

(d) Semisimple rings.

(e) $eRe$, where $e$ is an idempotent of the regular ring $R$.

(f) $\mathcal{M}_n(R)$, where $R$ is a regular ring.

31. (a) Show that regular rings have vanishing Jacobson radical, hence are semi-primitive. Give an example of a ring $R$ with $J(R) = 0$ that is not regular.

    (b) Show that the following conditions on a ring $R$ are equivalent:

    (i) $R$ is semisimple.

    (ii) $R$ is regular and artinian.

    (iii) $R$ is regular and noetherian.

32. Show that $R$ is regular if and only if every finitely generated submodule $M$ of a projective $R$-module $P$ is a direct summand. [Hint: for one direction take $R = P$; for the other, you may assume $P$ is free (why?). Then $Hom(P, M)$ is a left ideal of $\mathcal{M}_n(R)$ and is therefore a summand. So $M \approx Hom_R(R, M)$ is a projective $R$-module.]

### Clifford Algebras

Clifford algebras provide interesting examples of semisimple rings which generalize some of the rings we've studied, and are useful in differential geometry and the study of quadratic forms (see, e.g., Jacobson's *Basic Algebra I*).

Let $F$ be a field with characteristic not equal to 2, and let $a_1, \ldots, a_n$ be elements of $F$. The **Clifford algebra** $C = C(a_1, \ldots, a_n)$ is defined to be the free $F$-algebra $F\{x_1, \ldots x_n\}$ over indeterminates $x_1, \ldots x_n$ subject to the relations $x_i x_j = -x_j x_i$ and $x_i^2 = a_i$ for all $i \neq j$. For example, over the field $\mathbf{R}$ $C(-1)$ is the field $\mathbf{C}$ of complex numbers and $C(-1, -1)$ is the Quaternions $\mathbf{H}$. More generally, if $a_1$ and $a_2$ are nonzero elements of the field $F$, then $C(a_1, a_2)$ is the generalized quaternion algebra $\left(\frac{a_1, a_2}{F}\right)$ discussed in the exercises of Chapter 4. When all of the $a_i$'s are 0, $C$ is the **Grassmann algebra**, also known as the **exterior algebra**.

33. Which Clifford algebras have zero-divisors?

34. Let $C = C(a_1, \ldots, a_n)$ be a Clifford algebra. If $\{i_1, \ldots i_r\}$ is a subset of $N = \{1, 2, \ldots, n\}$ with $i_1 < i_2 < \cdots < i_r$, let $x_S$ denote the monomial $x_{i_1} x_{i_2} \cdots x_{i_r} \in C$. Show that $\{x_S : S \subseteq N\}$ is a basis for the Clifford algebra $C$, and hence $C$ has dimension $2^n$ over the field $F$; in particular $C$ is artinian.

35. (a) Let $C = C(a_1, \ldots, a_n)$ be a Clifford algebra. Prove that $C$ is semisimple if and only if $\prod_{i=1}^n a_i \neq 0$. [Hint: Necessity is easy. To prove sufficiency, use a trace argument which is similar to the proof of Maschke's Theorem given in Chapter 2, Exercise 32.]

(b) If $C$ is a Clifford algebra which is semisimple, show that $C$ is a direct sum of at most two simple components.

36. Let $C = C(a_1, \ldots a_n)$ be the clifford algebra with $a_i \neq 0$ if $i \leq r$ and $a_i = 0$ for $i > r$. Prove that $J(R)$ is generated by $x_{r+1}, \ldots, x_n$, and that $C/J(C) \approx C(a_1, \ldots, a_r)$.

### Classifying Quaternion Algebras

37. The goal of this group of exercises is to give a classification (as $F$-algebras) of the general quaternion algebras $\left(\frac{a,b}{F}\right)$ over the field $F$. We follow the treatment given in Pierce's *Associative Algebras*. For the definitions and basic properties of generalized quaternion algebras, see the section devoted to them in the exercises of Chapter 4. Recall that if $x = c_0 + c_1 i + c_2 j + c_3 k$ is an element of the generalized quaternion algebra $\left(\frac{a,b}{F}\right)$, then the **quaternion conjugate** of $x$ is defined to be $\overline{x} = c_0 - c_1 i - c_2 j - c_3 k$, and the **(quaternion) norm** of $x$ is defined to be $N(x) = x\overline{x} = c_0^2 - ac_1^2 - bc_2^2 - abc_3^2$.

38. Use the exercises on quaternion algebras in Chapter 4 to show that every generalized quaternion algebra over $\mathbf{R}$ is isomorphic (as an $\mathbf{R}$-algebra) to either $\mathbf{H}$ or $\mathcal{M}_2(\mathbf{R})$.

39. An element $x = c_0 + c_1 i + c_2 j + c_3 k$ of $A = \left(\frac{a,b}{F}\right)$ is called a **pure quaternion** if $c_0 = 0$. The set of pure quaternions is denoted by $A_0$. Show that the notion of pure quaternion is independent of the choice of basis for $A$ by showing that a nonzero element $x \in A$ is a pure quaternion if and only if $x \notin F$ and $x^2 \in F$.

40. Let $A = \left(\frac{a,b}{F}\right)$ and $A' = \left(\frac{a',b'}{F}\right)$ be generalized quaternion algebras with norms $N$ and $N'$, respectively. Show that $A$ and $A'$ are isomorphic (as $F$-algebras) if and only if there is a vector space isomorphism $\phi : A_0 \longrightarrow A_0'$ with $N'(\phi(x)) = N(x)$ for all $x \in A_0$.

41. Two quadratic forms $Q$ and $Q'$ on a vector space over a field $F$ are said to be **equivalent** if one may be obtained from the other by a change of basis. Represent $Q$ by the matrix $[Q_{ij}]$, so that

$$Q(x_1, x_2, x_3) = [x_1\ x_2\ x_3][Q_{ij}] \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

Then the quadratic forms $Q$ and $Q'$ are equivalent if and only if there is a non-singular matrix $P$ with $[Q_{ij}] = P^t[Q'_{ij}]P$, where $P^t$ denotes the transpose of $P$. Prove the following classification of quaternion algebras in terms of quadratic forms: The quaternion algebras $\left(\frac{a,b}{F}\right)$ and $\left(\frac{a',b'}{F}\right)$ are isomorphic (as $F$-algebras) if and only if the quadratic forms $Q(x_1,x_2,x_3) = ax_1^2+bx_2^2-abx_3^2$ and $Q'(x_1,x_2,x_3) = a'x_1^2+b'x_2^2-a'b'x_3^2$ are equivalent. [Hint: Let $Q(x_1,x_2,x_3) = -ax_1^2-bx_2^2+abx_3^2$. Note that if $x = c_1i+c_2j+c_3k$ is a pure quaternion, then $N(x) = Q(c_1,c_2,c_3)$; similarly for $Q'$ and $N'$. Write these equations in matrix form and see what Exercise 40 says.

42. Use the classification of quaternion algebras to show that $Br(\mathbf{Q})$ is infinite.

## Polynomial Identity Rings

For a deeper exploration of polynomial identity rings, see Procesi, *Rings with Polynomial Identities*, and Rowen, *Polynomial Identities in Ring Theory.*

Let $k$ be a field and let $k[x_1,\ldots,x_n]$ denote the free $k$-algebra in the (noncommuting) varibles $x_1,\ldots,x_n$. An algebra $A$ over $k$ is said to satisfy a **polynomial identity** if there exists a nonzero polynomial $f \in k[x_1,\ldots,x_n]$ for some $n$ such that $f(a_1,\ldots,a_n) = 0$ for all $a_1,\ldots,a_n$ in $A$. In this case $A$ is said to **satisfy** $f$, and $A$ is called a **polynomial identity algebra** , or **P.I. algebra** for short.

43. (a) Show that any commutative algebra is a P.I. algebra.

(b) Show that $\mathcal{M}_2(k)$ is a P.I. algebra over the field $k$.

(c) Let $S_n$ denote the group of permutations of $n$ objects, and let $sgn(\sigma)$ be 1 or $-1$ according to whether $\sigma$ is an even or odd permutation. In $k[x_1,\ldots,x_n]$, the **standard identity of degree** $n$ is

$$[x_1,\ldots,x_n] = \sum_{\sigma\in S_n} sgn(\sigma)x_{\sigma(1)}\cdots x_{\sigma(n)}$$

where $\sigma$ runs over all elements of $S_n$. Notice that $[x_1,x_2] = x_1x_2 - x_2x_1$. Show that if $A$ is an $n$-dimensional $k$-algebra then $A$ satisfies $[x_1,\ldots,x_{n+1}]$. Hence $\mathcal{M}_n(k)$ satisfies $[x_1,\ldots,x_{n^2+1}]$.

44. Let $n$ be a positive integer and let $f$ be a nonzero polynomial in $k[x_1,\ldots,x_n]$. Show that there exists an integer $m$ so that $\mathcal{M}_m(k)$ does not satisfy $f$. Thus there is no universal polynomial identity which holds for all matrix algebras.

45. (a) Show that if a $k$-algebra $A$ satisfies a polynomial identity of degree $d$ then it satisfies a multilinear identity whose degree is less than or equal to $d$. Conclude that if $A$ satisfies a multilinear identity $f$, then $A \otimes_k K$ satisfies $f$ for any extension field $K$ of $k$.

(b) Show that $\mathcal{M}_n(k)$ does not satisfy a polynomial identity of degree less than $2n$. [Hint: First show that if $\mathcal{M}_n(k)$ satisfies such an identity $f$, then one can assume that $f$ is multilinear and homogeneous.]

(c) Prove Kaplansky's Theorem, which is a cornerstone in the theory of P.I. rings: Let $A$ be a primitive algebra satisfying a polynomial identity of degree $d$. Then $A$ is a finite dimensional simple algebra over its center $Z(A)$, and the dimension of $A$ over $Z(A)$ is at most $[d/2]^2$, where $[d/2]$ denotes the greatest integer of $d/2$. [Hint: Use exercise 44 to show that $A$ is isomorphic to $\mathcal{M}_n(D)$ for some division ring $D$. Now split $D$ by a maximal subfield $K$, and show that $A \otimes_{Z(K)} K \approx \mathcal{M}_n(K)$. Now compute dimensions and apply parts (a) and (b) to obtain the desired conclusion.]

**Final Exam**

46. Some Rings:

(a) $\mathbf{Z}$
(b) $\mathbf{Z}/n\mathbf{Z}$
(c) $\mathbf{C}[x]$
(d) $\mathbf{C}[x, y]$
(e) $\mathbf{Q}[x]/(x^3 - 5x)$
(f) $\mathbf{C}[x, y]/(2x^2 - y^2 + 1)$
(g) $\mathcal{M}_n(\mathbf{R})$
(h) $\mathcal{T}_n(\mathbf{R})$, the ring of upper triangular matrices.
(i) $\mathbf{C}[[x]]$, the ring of formal power series over $\mathbf{C}$
(j) $\mathbf{C}[x, x^{-1}]$, the ring of formal Laurent series over $\mathbf{C}$
(k) $\mathbf{C}[G]$, where $G$ is a cyclic group
(l) $\mathbf{C}[G]$, where $G$ is any finite group
(m) The ring of real-valued continuous functions on $[0, 1]$
(n) A twisted polynomial ring (cf. Chapter 2, Exercise 9)

For each of the rings listed above, determine whether that ring is

(a) simple
(b) semisimple

(c) radical free, i.e. $J(R) = 0$

(d) artinian

(e) noetherian

(f) primitive

(g) semi-primitive

(h) prime

(i) von Neumann regular

For each of the rings $R$ listed above, compute the following :

(a) $Z(R)$

(b) $J(R)$

(c) The units of $R$

(d) The zero-divisors of $R$

(e) The nilpotent elements of $R$

(f) The idempotents of $R$

For each of the rings $R$ listed above, classify the finitely generated $R$-modules which are:

(a) simple

(b) semisimple

(c) of finite length

(d) free

(e) projective

(f) injective

# References


Albert, A.A., *Structure of Algebras*, AMS. Coll. Publ. 24, 1939.

Amitsur, S., "On Central Division Algebras", *Israel J. Math.* 12 (1972), pp. 408-420.

Artin, E., *Geometric Algebra*, Interscience, New York, 1957.

Atiyah, M. and I. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Pub. Co., Reading, Mass., 1969.

Auslander, M. and O. Goldman, "The Brauer Group of a Commutative Ring", *T.A.M.S.*, Vol. 97, No. 3, 1960.

Bass, H., *Algebraic K-Theory*, W.A. Benjamin, Inc., New York, 1968.

Bass, H., *Topics in Algebraic K-Theory*, Lectures in Mathematics and Physics No. 41, Tata Institute of Fundamental Research, Bombay, 1967.

Bourbaki, N., *Élements de Mathématique*, Vol. I, Livre II, Chap. 8, Hermann, Paris, 1958.

Burnside, W., "On groups of order $p^\alpha q^\beta$", *Proc. London Math Soc.* (2), 2 (1904), pp.432-437.

Chase, S., "Two Remarks on Central Simple Algebras", *Comm. in Algebra*, 12, 1984, pp.2279-2289.

Chase, S., Harrison, D. and A. Rosenberg, *Galois Theory of Commutative Rings*, Memoirs of the A.M.S., No.52 (1965).

Curtis, C. and I. Reiner, *Methods of Representation Theory*, Vol. I, John Wiley and Sons, New York, 1981.

DeMeyer, F. and E. Ingraham, *Separable Algebras Over Commutative Rings*, Lecture Notes in Mathematics, Vol. 181, Springer-Verlag, New York, 1970.

Deuring, M., *Algebren*, Erg. der Math. Band 4, Springer-Verlag, Berlin, 1935.

Dickson, L., *Algebras and Their Arithmetics*, University of Chicago Press, Chicago, 1923.

Divinsky, N.J., *Rings and Radicals*, Mathematical Expositions 14, Allen and Unwin, London, 1965.

Fulton, W. and J. Harris, *Representation Theory : A First Course*, Graduate Texts in Math., Readings in Math., Springer-Verlag, New York, 1991.

Goldschmidt, D., "A group theoretic proof of the $p^\alpha q^\beta$ theorem, for odd primes", *Math Z.*, 113 (1970),pp.373-375.

Gorenstein, D., *Finite Groups*, Harper and Row, New York, 1968.
Gray, M., *A Radical Approach To Algebra*, Addison-Wesley Pub. Co., Reading, Mass., 1970.
Grothendieck, A., "Le Groupe de Brauer, I, II, III", in *Dix exposés sur la cohomologie des schémas*, North-Holland Pub. Co., Amsterdam, 1968.
Halmos, P., *Naive Set Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1974.
Herstein, I.N., *Noncommutative Rings*, Carus Mathematical Monographs, No. 15, 1968.
Jacob, B. and A. Wadsworth, "A new construction of noncrossed product algebras", *T.A.M.S.* 293, pp.693-721.
Jacobson, N., *Basic Algebra I, II*, W.H. Freeman and Company, San Francisco, 1980.
Jans, J.P., *Rings and Homology*, Holt, Rinehart and Winston, 1964.
Jategaonkar, A., "A counter-example in ring theory and homological algebra", *J. Algebra* 12 (1969),pp.418-440.
Kaplansky, I., *Fields and Rings*, University of Chicago Press, 1969.
Kaplansky, I., *Global Dimension of Rings*, Queen Mary College Notes.
Kaplansky, I., "Projective Modules",*Math. Ann.*, 68 (1958), pp. 372-377.
Kersten, I. *Brauergruppen von Körpern*, Aspects of Mathematics, Friedr. Vieweg und Sohn, Braunschweig, 1990.
Lam, T.Y., *The Algebraic Theory of Quadratic Forms*, W.A. Benjamin, Inc., 1973.
Matsumaya, H., "Solvability of groups of order $2^a p^b$", *Osaka J. Math*, 10 (1973), pp.375-378.
Milnor, J., *Introduction to Algebraic K-Theory*, Annals of Mathematic Studies, Princeton University Press, 1971.
Orzech, M. and L. Small, *The Brauer Group of Commutative Rings*, Lecture Notes in Pure and Applied Mathematics, Marcel Dekker, Inc., New York, 1975.
Passman, D., *A Course in Ring Theory*, Wadsworth and Brooks/Cole, Pacific Grove, California, 1991.
Passman, D., "Advances in Group Rings", *Israel J. Math.* 19, 1974, pp.67-107.
Pierce, R.S.,*Associative Algebras*,Graduate Texts in Mathematics, Springer-Verlag, New York, 1982.
Procesi, C., *Rings with Polynomial Identities*, Marcel Dekker, New York, 1973.
Reiner, I., *Maximal Orders*, Academic Press, New York, 1975.
Rotman, J., *An Introduction to Homological Algebra*, Academic Press, New York, 1979.
Rotman, J., *An Introduction to the Theory of Groups*, Allyn and Bacon, Inc., 1984.
Rowen, L., *Ring Theory*, Vols. I and II, Academic Press, 1988.

Rowen, L., *Polynomial Identities in Ring Theory*, Academic Press, New York, 1980.

Samuel, P., *Algebraic Theory of Numbers*, translated from the French by A. Silberger, Houghton Mifflin Co., Boston, 1970.

Serre, J.P., *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer-Verlag, New York, 1973.

Serre, J.P., *Linear Representations of Finite Groups*, translated from the French by L. Scott, Graduate Texts in Mathematics, No. 42, Springer-Verlag, New York, 1977.

Serre, J.P., *Local Fields*, translated from the French by M. Greenberg, Graduate Texts in Mathematics 67, Springer-Verlag, New York, 1979.

Zalesskii, A. and A. Mikhalev, "Group Rings", *J. Soviet Math.* 4, 1975, pp.1-78.

Zelinsky, D., "Brauer Groups", in *Ring Theory II : Proceedings of the Second Oklahoma Conference*, B. McDonald and R. Morris, Eds., Lecture Notes in Mathematics 26, pp.69-102, Marcel Dekker, New York.

# Index

# Graduate Texts in Mathematics

*continued from page ii*

48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG. A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. $p$-adic Numbers, $p$-adic Analysis, and Zeta-Functions. 2nd ed.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.
61 WHITEHEAD. Elements of Homotopy Theory.
62 KARGAPOLOV/MERLZJAKOV. Fundamentals of the Theory of Groups.
63 BOLLOBAS. Graph Theory.
64 EDWARDS. Fourier Series. Vol. I. 2nd ed.
65 WELLS. Differential Analysis on Complex Manifolds. 2nd ed.
66 WATERHOUSE. Introduction to Affine Group Schemes.
67 SERRE. Local Fields
68 WEIDMANN. Linear Operators in Hilbert Spaces.
69 LANG. Cyclotomic Fields II.
70 MASSEY. Singular Homology Theory.
71 FARKAS/KRA. Riemann Surfaces. 2nd ed.
72 STILLWELL. Classical Topology and Combinatorial Group Theory. 2nd ed.
73 HUNGERFORD. Algebra.
74 DAVENPORT. Multiplicative Number Theory. 2nd ed.
75 HOCHSCHILD. Basic Theory of Algebraic Groups and Lie Algebras.
76 IITAKA. Algebraic Geometry.
77 HECKE. Lectures on the Theory of Algebraic Numbers.
78 BURRIS/SANKAPPANAVAR. A Course in Universal Algebra.
79 WALTERS. An Introduction to Ergodic Theory.
80 ROBINSON. A Course in the Theory of Groups.
81 FORSTER. Lectures on Riemann Surfaces.
82 BOTT/TU. Differential Forms in Algebraic Topology.
83 WASHINGTON. Introduction to Cyclotomic Fields.
84 IRELAND/ROSEN. A Classical Introduction to Modern Number Theory. 2nd ed.
85 EDWARDS. Fourier Series. Vol. II. 2nd ed.
86 VAN LINT. Introduction to Coding Theory. 2nd ed.
87 BROWN. Cohomology of Groups.
88 PIERCE. Associative Algebras.
89 LANG. Introduction to Algebraic and Abelian Functions. 2nd ed.
90 BRONDSTED. An Introduction to Convex Polytopes.
91 BEARDON. On the Geometry of Discrete Groups.
92 DIESTEL. Sequences and Series in Banach Spaces.
93 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry--Methods and Applications. Part I. 2nd ed.
94 WARNER. Foundations of Differentiable Manifolds and Lie Groups.
95 SHIRYAYEV. Probability, Statistics, and Random Processes.
96 CONWAY. A Course in Functional Analysis.

97 KOBLITZ. Introduction to Elliptic Curves and Modular Forms. 2nd ed.
98 BRÖCKER/TOM DIECK. Representations of Compact Lie Groups.
99 GROVE/BENSON. Finite Reflection Groups. 2nd ed.
100 BERG/CHRISTENSEN/RESSEL. Harmonic Analysis on Semigroups: Theory of Positive Definite and Related Functions.
101 EDWARDS. Galois Theory.
102 VARDARAJAN. Lie Groups, Lie Algebras and Their Representations.
103 LANG. Complex Analysis. 2nd ed.
104 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry--Methods and Applications. Part II.
105 LANG. $SL_2(\mathbf{R})$.
106 SILVERMAN. The Arithmetic of Elliptic Curves.
107 OLVER. Applications of Lie Groups to Differential Equations. 2nd ed.
108 RANGE. Holomorphic Functions and Integral Representations in Several Complex Variables.
109 LEHTO. Univalent Functions and Teichmüller Spaces.
110 LANG. Algebraic Number Theory.
111 HUSEMÖLLER. Elliptic Curves.
112 LANG. Elliptic Functions.
113 KARATZAS/SHREVE. Brownian Motion and Stochastic Calculus. 2nd ed.
114 KOBLITZ. A Course in Number Theory and Cryptography.
115 BERGER/GOSTIAUX. Differential Geometry: Manifolds, Curves, and Surfaces.
116 KELLEY/SRINIVASAN. Measure and Integral. Vol. I.
117 SERRE. Algebraic Groups and Class Fields.
118 PEDERSEN. Analysis Now.
119 ROTMAN. An Introduction to Algebraic Topology.
120 ZIEMER. Weakly Differentiable Functions: Sobolev Spaces and Functions of Bounded Variation.
121 LANG. Cyclotomic Fields I and II. Combined 2nd ed.
122 REMMERT. Theory of Complex Functions.
*Readings in Mathematics*
123 EBBINGHAUS/HERMES et al. Numbers.
*Readings in Mathematics*
124 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry--Methods and Applications. Part III.
125 BERENSTEIN/GAY. Complex Variables: An Introduction.
126 BOREL. Linear Algebraic Groups.
127 MASSEY. A Basic Course in Algebraic Topology.
128 RAUCH. Partial Differential Equations.
129 FULTON/HARRIS. Representation Theory: A First Course.
*Readings in Mathematics*
130 DODSON/POSTON. Tensor Geometry.
131 LAM. A First Course in Noncommutative Rings.
132 BEARDON. Iteration of Rational Functions.
133 HARRIS. Algebraic Geometry: A First Course.
134 ROMAN. Coding and Information Theory.
135 ROMAN. Advanced Linear Algebra.
136 ADKINS/WEINTRAUB. Algebra: An Approach via Module Theory.
137 AXLER/BOURDON/RAMEY. Harmonic Function Theory.
138 COHEN. A Course in Computational Algebraic Number Theory.
139 BREDON. Topology and Geometry.
140 AUBIN. Optima and Equilibria. An Introduction to Nonlinear Analysis.
141 BECKER/WEISPFENNING/KREDEL. Gröbner Bases. A Computational Approach to Commutative Algebra.
142 LANG. Real and Functional Analysis. 3rd ed.
143 DOOB. Measure Theory and Probability.
144 DENNIS/FARB. Noncommutative Algebra.
145 VICK. Homology Theory. 2nd ed.